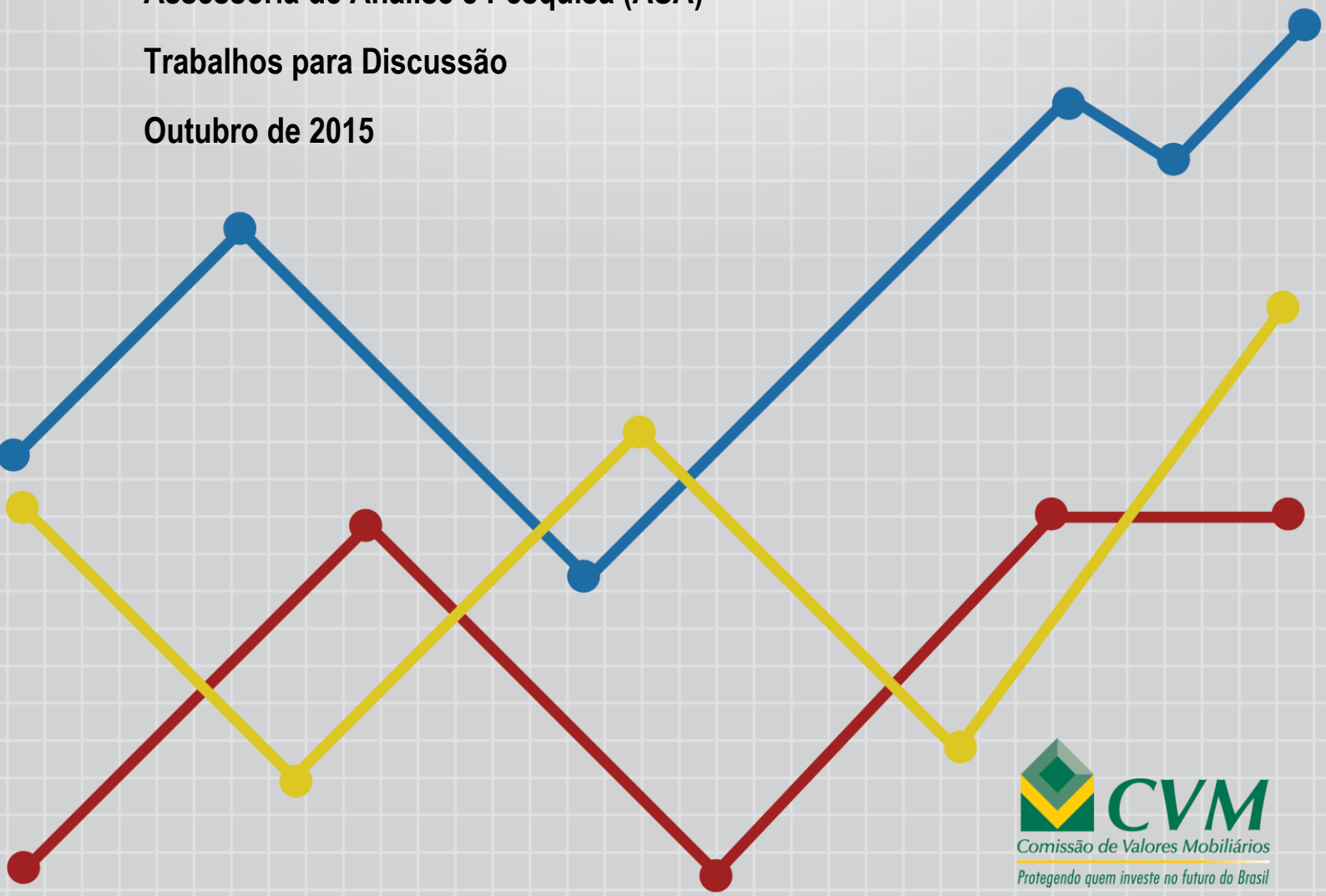
Gerenciamento de riscos corporativos:

uma análise das diretrizes e das práticas

Assessoria de Análise e Pesquisa (ASA)

Trabalhos para Discussão

Outubro de 2015



CVM
Comissão de Valores Mobiliários
Protegendo quem investe no futuro do Brasil

Elaboração: Equipe ASA

Contato: asa@cvm.gov.br

Este estudo expressa as opiniões e conclusões de seus autores e não necessariamente as da Comissão de Valores Mobiliários.

O presente estudo beneficiou-se de importantes comentários feitos pela Superintendência de Empresas (SEP) e pela Superintendência de Normas Contábeis e de Auditoria (SNC), a quem agradecemos. Ele expressa as opiniões e conclusões de seus autores e não necessariamente as da Comissão de Valores Mobiliários.

Índice

Sumário Executivo

Embora a ideia de governança corporativa seja muito antiga, o termo "governança corporativa" em si passou a ser disseminado somente nos anos 80 do século passado, tendo o surgimento dos primeiros códigos de melhores práticas de governança corporativa ocorrido apenas nos anos 90.

Mais recente ainda é o entendimento sobre o papel do conselho de administração no gerenciamento de riscos, para além dos conceitos de conformidade e *compliance*. A OCDE, em seus estudos, considera que o tema não está devidamente coberto nos códigos de governança corporativa em vigência. De fato, numa revisão dos padrões de gerenciamento de riscos em 27 países, publicada em 2014, a OCDE aponta que os padrões existentes para companhias listadas continuam centradas nas funções de auditoria e controles internos, e primariamente em riscos financeiros.

Sendo assim, em virtude do recente desenvolvimento do tema no contexto de governança, e de considerações de que há espaço para os códigos de governança ou os reguladores endereçarem melhor "gerenciamento de riscos", o objetivo deste nosso trabalho consiste em verificar eventuais lacunas que, se trabalhadas, possam materializar melhor as recomendações/requisitos existentes na regulamentação ou nos códigos brasileiros. Mais precisamente, o nosso estudo visa a contribuir com os debates sobre o futuro Código Brasileiro de Governança Corporativa (Pratique ou Explique), que está sendo elaborado pelo Grupo Interagentes.

Para tanto, além do capítulo introdutório, contextualizando as discussões e o objetivo do trabalho, o presente relatório é composto por outros quatro capítulos. O Capítulo 2 contém uma revisão bibliográfica sobre a diferenciação entre gerenciamento de riscos, controles internos e *compliance*, além de abordar o papel do conselho de administração e estudos empíricos relacionados à geração de valor. O Capítulo 3 apresenta um levantamento sobre as diretrizes em outros países, bem como algumas práticas que materializam o gerenciamento de riscos. No capítulo 4 são apresentadas a regulamentação da CVM a respeito do tema e as previsões existentes nos dois códigos de governança atualmente existentes no Brasil. E no capítulo 5, tem-se a conclusão.

No Capítulo 2, mostramos que, ainda que haja visões diferentes sobre gerenciamento de riscos, conforme apresentadas na revisão de literatura realizada, podemos afirmar resumidamente que:

- *Compliance* (aderência às normas e procedimentos definidos previamente) tende a ser visto na literatura como parte, seja de gerenciamento de riscos, seja apenas de controles internos, ambos com escopo mais amplo dentro da empresa.
- A função de controles internos pode ser compreendida como tendo intersecção com um sistema de gerenciamento de riscos. O sistema de controles internos, além de *compliance*, busca assegurar que as operações da empresa sigam conforme o planejado, mitigando desvios, e, embora não questione aquilo que foi planejado, pode contribuir de forma crítica. Nem todas as atividades da função controles internos (operacional) endereçam "riscos" e nem todo controle de riscos relevantes pode ser tratado por meio da função de controles internos.
- Gerenciamento de riscos é mais holístico, ao se inserir não só nos contornos das operações, mas também no direcionamento estratégico da organização, incorporando diferentes perspectivas, tais como o ambiente externo e a reputação da organização. Também, gerenciamento de riscos é mais amplo, incluindo o processo de identificação, mensuração (qualitativa ou quantitativa), avaliação de riscos, bem como a definição da atitude da organização perante estes riscos e os seus tratamentos (inclusive controle).

O capítulo ressalta ainda que, embora a palavra "riscos" possa ter uma conotação negativa, há respaldo na literatura para a ideia de que o gerenciamento de riscos não requer que os riscos deixem de ser incorridos. A ideia é que os mesmos sejam compreendidos, gerenciados e, quando pertinente, comunicados. Nesse sentido, um bom gerenciamento de riscos pode, inclusive, implicar a *elevação* do grau de risco incorrido por uma empresa em busca de seus objetivos.

Um dos desdobramentos da visão estratégica do gerenciamento de riscos consiste no debate sobre a responsabilidade sobre sua formulação, definição e/ou aprovação, incluindo os órgãos dentro da empresa que devem ter essa responsabilidade e o escopo da responsabilidade desses órgãos.

A formulação pode ocorrer de forma autônoma nas diversas áreas/departamentos/unidades organizacionais, em que cada uma delas considera seus próprios objetivos e parâmetros (modelo de silos fechados), ou então de forma integrada, havendo coordenação de visão dentro da organização. Esse assunto é tratado extensivamente na literatura e a tendência tem sido pela integração. De uma forma mais geral, ao envolver a estratégia das organizações e as interações entre as diversas áreas, torna-se razoável supor que o gerenciamento de riscos requer uma formulação a nível organizacional, não apenas sub-organizacional, muito embora a execução dos processos ocorra em diversos níveis.

Assim, ao compreender o gerenciamento de riscos como essencial para atingir os objetivos da empresa, inclusive os estratégicos, também se torna razoável atribuir essa responsabilidade ao órgão responsável pelo direcionamento e pelas decisões estratégicas da empresa. Conforme apresentado neste estudo, os Princípios de Governança Corporativa da OCDE conferem responsabilidades finais de desenho, supervisão e monitoramento dos sistemas de gerenciamento de riscos corporativos aos conselhos de administração e seus comitês.

O Capítulo 2 é complementado pela apresentação de alguns estudos empíricos sobre o gerenciamento de riscos e geração de valor. Alguns deles são mais gerais e versam sobre a relação entre a estrutura organizacional de gerenciamento de riscos e seus impactos sobre as métricas de risco, enquanto que outros são mais específicos e lidam apenas com a eficácia de determinados mecanismos de gerenciamento de riscos financeiros.

Com base nesses estudos, pode-se dizer que há justificativas teóricas para a adoção do gerenciamento de riscos corporativos em termos de geração de valor (incluso gerenciamento de riscos financeiros), bem como evidências empíricas. Entretanto, não há unanimidade nos resultados empíricos, constatação para a qual se deve levar em conta as limitações dos métodos quantitativos nas ciências sociais e a dificuldade de mensuração das variáveis de gerenciamento de riscos.

Apesar da concepção de gerenciamento de riscos estar relacionada com governança corporativa ser relativamente nova, já podem ser encontrados diversos dispositivos em outras jurisdições, sejam eles regulamentações ou códigos de governança "*comply or explain"*, conforme pode ser visto no Capítulo 3. Nele é apresentado um levantamento sobre as diretrizes em outros países, bem como algumas práticas que materializam o gerenciamento de riscos e diversas pesquisas mostrando o seu estágio de implementação nas empresas.

No que diz respeito a princípios gerais, foram analisados em especial os princípios da OCDE e uma amostra de 21 códigos de melhores práticas de governança corporativa (incluindo dois códigos brasileiros, o do IBGC – 4ª edição e o da Abrasca). Dentre os destaques, cita-se que, na quase totalidade dos casos, há atribuição de algum nível de responsabilidade ao conselho de administração, seja na formulação/aprovação/revisão de políticas e mecanismos de gerenciamento de risco, seja no monitoramento de sua execução pelo corpo gestor. Por fim, a tônica geral é a de que os códigos não são muito prescritivos.

Em relação a diretrizes mais específicas, menciona-se no Capítulo 3 o ISO 31000 que, por seu papel de estabelecer padrões internacionais, aponta não só princípios, mas também práticas gerais, com o intuito de tornar o gerenciamento de riscos mais operacional.

No ISO 31000, a estrutura conceitual de gerenciamento de riscos é entendida como o *conjunto de componentes que fornecem as fundações (política, objetivos, mandato e comprometimento para administrar o risco) e os arranjos organizacionais (planos, relações, responsabilidades, recursos, processos e atividades) por desenhar, implementar, monitorar, revisar e melhorar continuamente as atividades coordenadas para direcionar e controlar uma organização no que refere a riscos*.

Assim, no intuito de apontar algumas diretrizes que materializem melhor "gerenciamento de riscos", destacamos naquele capítulo:

- Mandato e comprometimento: necessidade de atribuir a responsabilidade sobre o *framework* à alta administração, conselho e/ou gestores, para que haja comprometimento de toda organização. Assim, a alta administração é responsável por desenhar, implementar, monitorar, revisar e melhorar continuamente o gerenciamento de riscos, ressaltando-se a responsabilidade pela definição e o endosso da política de gerenciamento de riscos e pelo alinhamento dos objetivos do gerenciamento de riscos com os objetivos e estratégias da organização.
- Desenho do *framework*: necessidade do entendimento prévio sobre os contextos interno e externo; o estabelecimento de mecanismos de comunicação e reporte; e a formulação da política de gerenciamento de riscos. A política de gerenciamento de risco é definida no ISO 31000 como a declaração da organização sobre as intenções e direcionamento gerais em relação ao gerenciamento de riscos. Mais concretamente, a política, geralmente, inclui o racional da organização para administrar riscos; a ligação entre os objetivos da organização e a política de gerenciamento; as responsabilidades dos diversos órgãos e níveis da empresa; a forma em que o desempenho de todo o sistema de gerenciamento de riscos é mensurado, além de seu reporte, e o comprometimento de disponibilizar recursos às atividades, de revisar e melhorar a política e o *framework* de gerenciamento de riscos.
- Implementação de gerenciamento de riscos: referência à implementação do processo. O processo é entendido como a aplicação sistemática de políticas, procedimentos e práticas nas atividades de comunicação, consulta e estabelecimento de contexto, assim como nas atividades de identificação, análise, avaliação, tratamento, monitoramento e revisão de riscos. No estabelecimento do contexto, a organização considera os seus objetivos e define os parâmetros (internos e externos) na administração de riscos, além de definir os critérios de risco para avaliar a significância de um risco.
- Monitoramento e revisão do *framework*: inclui a mensuração do desempenho e do progresso de gerenciamento de riscos, respectivamente, em relação a indicadores e aos planos de gerenciamento de risco; reporte sobre riscos, progressos na execução do plano e da política de gerenciamento de riscos, e revisão do *framework*, política e planos de gerenciamento de riscos.
- Melhoria contínua do *framework*: refere-se às decisões sobre como o *framework*, a política e os planos de ação podem ser melhorados.

Mesmo existindo importantes diretrizes, há evidências de que a adoção do gerenciamento de riscos não está plenamente disseminada. Em especial, uma recente pesquisa global conduzida pela seguradora AON (2015) fornece indicações nesse sentido. A pesquisa foi realizada no último trimestre de 2014, com 1418 empresas clientes (publicamente negociadas ou não).

Segundo a pesquisa, em 24% das empresas analisadas, o conselho de administração ou um de seus comitês não havia estabelecido (ou não sabia informar) política de gerenciamento de riscos, ainda que informais - esse percentual tende a cair conforme o faturamento da empresa se eleva.

Na sequência, no capítulo 4 são apresentadas principalmente a regulamentação da CVM a respeito do tema e as previsões existentes nos códigos do IBGC e da Abrasca.

Em resumo, as normas da CVM demandam amplo *disclosure* dos principais riscos financeiros e não financeiros. Em relação a gerenciamento de riscos, há a solicitação de informação sobre a existência de uma política formalizada ou não (inclusive a explicação das razões, caso não houver); o órgão responsável pela sua aprovação, bem como os objetivos e as estratégias dessa política, incluindo os riscos para os quais se busca a proteção, os instrumentos utilizados na proteção e como o gerenciamento de riscos se estrutura na organização. Adicionalmente é solicitada a informação de como a estrutura operacional e de controles internos está adequada para verificar a efetividade da política de gerenciamento. No que refere a controles internos no âmbito de elaboração de demonstrações contábeis confiáveis, além de amplo *disclosure*, há normas específicas sobre o assunto.

Enquanto que as normas da CVM referentes a gerenciamento de riscos tratam de *disclosure*, os dois códigos atualmente existentes no Brasil têm caráter de fornecer diretrizes ou recomendações, principalmente em relação à responsabilidade dos órgãos de administração. O código de IBGC constitui tem caráter de um guia de boas práticas de governança, enquanto que o código da Abrasca tem o formato de "Pratique ou Explique".

Apesar de haver similaridade em alguns pontos, aparentemente há diferenças na intensidade de foco e de envolvimento do conselho de administração no desenvolvimento do gerenciamento de riscos. Por exemplo, o código do IBGC dá a entender um envolvimento maior do conselho, ao indicar que este órgão deve estabelecer as diretrizes e as políticas de gerenciamento de riscos, enquanto que, no da Abrasca, a tarefa do conselho é o de aprovação da política. Também, o código do IBGC aponta que o conselho deve aprovar políticas específicas de limites para os principais riscos, ao mesmo tempo em que o da Abrasca cita riscos operacionais e financeiros.

Destaca-se que ambos os códigos indicam a diretoria como responsável pela execução de gerenciamento de riscos e controles internos, por meio de construção de sistemas para tais finalidades. Vale também mencionar que o conceito de controles internos em ambos os códigos vai além daqueles que incluem apenas controles internos direcionados para a preparação confiável de informações financeiras.

Finalmente, no Capítulo 5, concluímos, afirmando que os códigos de governança existentes atualmente no Brasil alinham-se com os Princípios da OCDE no que tange a gerenciamento de riscos. Os princípios da OCDE especificam o conselho de administração da empresa como responsável por direcionar, monitorar e revisar as políticas e procedimentos de gerenciamento de riscos, bem como por assegurar a integridade dos reportes contábeis e financeiros e a existência de controles internos adequados. Ao mesmo tempo, os princípios deixam claro que o corpo executivo é responsável por administrar os riscos. Ainda, os princípios da OCDE apontam a necessidade de se estabelecer o grau de risco aceito pela empresa frente aos seus objetivos e como esta irá gerenciar os riscos inerentes a suas operações e relações.

Princípios são diretrizes gerais essenciais, porém, há a necessidade de materializá-los em práticas operacionais mais concretas para que possam ser úteis tanto para as empresas quanto para a informação direcionada aos investidores.

Assim, dado que este trabalho busca verificar eventuais lacunas que, se trabalhadas, poderiam contribuir para aperfeiçoamentos no *disclosure* que a CVM já requer das empresas, mas principalmente visa a contribuir para os debates do futuro Código Brasileiro de Governança Corporativa (Pratique ou Explique), chamamos atenção, na conclusão, para a necessária clarificação entre os papéis de controles internos, *compliance* e gerenciamento de riscos. Independentemente de como a empresa se organiza, ao se dar o *disclosure*, é preciso algum direcionamento sobre o que deve ser considerado em cada uma dessas funções, por exemplo, na forma como fez o Formulário de Referência da ICVM 480, especificando alguns elementos sobre política de gerenciamento de riscos em sua seção 5.

Outro ponto de atenção é a indicação de práticas mínimas que devem ser atendidas para a empresa afirmar que adota gerenciamento de riscos (incorporando parte dos controles internos que nos interessa no estudo), de forma que os investidores possam fazer uma melhor avaliação sobre os principais riscos e as práticas da empresa. Contudo, como buscamos alertar ao longo do texto, as empresas são diferentes entre si, o que significa que, diante das suas particularidades, muito possivelmente se estruturam de forma diferente para gerenciar riscos.

Uma vez que o conteúdo do Código do IBGC será utilizado como base do futuro Código Brasileiro de Governança Corporativa (Pratique ou Explique), e que possivelmente o Formulário de Referência será utilizado como veículo de reporte para as empresas, o capítulo final apresenta uma comparação entre algumas diretrizes/práticas mostradas ao longo do estudo e os tópicos correspondentes no Código do IBGC e na ICVM 480. Finalmente, por meio de comentários, concluímos sobre as lacunas que a nosso ver poderiam ser preenchidas, tendo em vista o Código Brasileiro de Governança Corporativa.

1. Introdução

Embora a ideia de governança corporativa seja muito antiga, o termo "governança corporativa" em si passou a ser disseminado somente nos anos 80 do século passado (Tricker, 2015, p.4), tendo aparecido, pela primeira vez, no diário oficial dos EUA em 1976 (Cheffins, 2013, p.2). O surgimento de códigos de melhores práticas de governança corporativa, centrados no papel do conselho de administração e na governança dentro das empresas para proteger os direitos dos acionistas, ocorreu nos anos 90: o primeiro deles, The UK Corporate Governance Code[1], foi produzido em 1992 pelo Cadbury Committee.

Mais recente é o entendimento sobre o papel do conselho de administração no gerenciamento de riscos, para além dos conceitos de conformidade e *compliance*. De acordo com Tricker (2015, p.14), num posicionamento avançado para a época, em 1993, um comitê australiano de governança corporativa apontou a sua dimensão estratégica, relacionando o gerenciamento de riscos com a agregação de valor. Nas palavras daquele comitê, "*the board's key role is to ensure that corporate management is continously and effectively striving for above average performance, taking account to risk".*[2]

Em seu estudo, Enriques & Zetzsche (2013, p.7-10) identificam quatro ondas regulatórias europeias no que tange a gerenciamento de riscos. A primeira, em 1989, decorreu do acordo de Basiléia I. A segunda onda, ocorrida nos anos 90, focou nas empresas não financeiras, após os problemas com a alemã Metallgesellschaft. A terceira foi aquela do início dos anos 2000, como resposta aos escândalos da Enron e Parmalat.

Com a crise financeira global de 2007/2008 (quarta onda), o tema foi colocado em evidência novamente. Segundo apontado em estudo da OCDE[3], o gerenciamento de risco nas empresas do setor financeiro foi considerado ineficiente, e, embora não tenha sido o motivo, pode ter facilitado a ocorrência da crise (Kirkpatrick, 2009, p.31).

O mesmo estudo considera que o tema gerenciamento de riscos não está devidamente coberto nos códigos de governança corporativa em vigência (*idem*, p.9). De fato, numa revisão dos padrões de gerenciamento de riscos em 27 países, publicada em 2014, (OCDE, 2014, p.7), a OCDE, além de indicar que as diretrizes atuais são genéricas demais para serem aplicáveis na prática, aponta que os padrões existentes para companhias listadas continuam centradas nas funções de auditoria e controles internos, e primariamente em riscos financeiros, ao invés de identificação *ex-ante* dos riscos e de seu gerenciamento abrangente (*idem*, p.7).

Assim, de acordo com o relatório da OCDE, há escopo para a definição de padrões mais operacionais, sem, no entanto, penalizar a necessária flexibilidade de serem aplicáveis a diferentes empresas e situações (*ibidem*), por exemplo, a indicação sobre riscos potencialmente catastróficos ou aqueles que têm fortes impactos negativos para os investidores, partes relacionadas e/ou a sociedade.

Em relação a esta quarta onda, Enriques & Zetzsche (2013, p.10) ressaltam que, sob a perspectiva dos reguladores, teria havido uma ampliação do foco em relação a gerenciamento de riscos. Além de ser visto como mecanismo de autopreservação para o benefício das empresas e de seus acionistas, o

[1] Anteriormente, chamado de "The Combined Code on Corporate Governance".
[2] Segundo Tricker (2015, p.194), o Cadbury Committee, em 1992, também pregava o envolvimento do conselho com o gerenciamento de riscos. No entanto, restringia-se a riscos financeiros.
[3] Organização para Cooperação e Desenvolvimento Econômico.

gerenciamento de riscos passa a ser visto também como um mecanismo para direcionar o mercado e como medida de controle de riscos sistêmicos para o benefício das partes interessadas.

Em virtude do recente desenvolvimento do tema e das considerações de os códigos de governança ou os reguladores não estarem adentrando suficientemente o tópico "gerenciamento de riscos", desde o seu escopo até a governança, o objetivo deste nosso trabalho, à luz das discussões que têm ocorrido, consiste em verificar lacunas que, se trabalhadas, poderiam materializar melhor as recomendações/requisitos existentes na regulamentação ou nos códigos brasileiros. Mais especificamente, pretende contribuir para aperfeiçoamentos no *disclosure* que a CVM já requer das empresas, mas principalmente visa a contribuir para os debates do futuro Código Brasileiro de Governança Corporativa, que está sendo elaborado pelo Grupo Interagentes. [4]

Para tanto, além desta Introdução, o trabalho é composto por outros quatro capítulos. O capítulo 2 contém uma revisão bibliográfica sobre a diferenciação entre gerenciamento de riscos, controles internos e compliance, além do papel do conselho de administração e de estudos empíricos relacionados à geração de valor em função de adoção de gerenciamento de riscos. O capítulo 3 apresenta um levantamento sobre as diretrizes em outros países, bem como algumas práticas que materializam o gerenciamento de riscos e o estágio de implementação nas empresas. No capítulo 4 são apresentadas a regulamentação da CVM a respeito, as previsões existentes nos códigos do IBGC[5] e da Abrasca[6] e a compilação de algumas práticas de empresas brasileiras, conforme reportadas em Formulário de Referência para a CVM. Finalmente, no capítulo 5 tem-se a conclusão.

[4] O Grupo Interagentes é formado por 11 entidades (ANBIMA, ABRAPP, ABRASCA, ABVCAP, AMEC, APIMEC, BMF&BOVESPA, BRAiN, IBGC, INSTITUTO IBMEC e IBRI), além de ter a CVM e o BNDES como membros observadores. O Código Brasileiro de Governança Corporativa está sendo elaborado no formato "Pratique ou Explique" e há intenção de que a sua adoção seja obrigatória, ao menos, para as empresas com ações negociadas em bolsa.
[5] Instituto Brasileiro de Governança Corporativa.
[6] Associação Brasileira das Companhias Abertas.

2. Revisão bibliográfica

2. Definições e evolução do gerenciamento de riscos

2.1.1. *Compliance* versus controles internos versus gerenciamento de riscos

Primeiramente, faz-se necessário em nossa revisão de literatura abordar a distinção entre gerenciamento de riscos, controles internos e compliance, uma vez que os três conceitos são utilizados, algumas vezes, como sinônimos, particularmente "gerenciamento de riscos" e "controles internos".

Miller (2014, p.1) distingue *compliance* de controles internos. *Compliance*, para ele, encontra-se sob o guarda-chuva dos controles internos, e consiste nos esforços da organização para assegurar que os seus colaboradores não violem as regras, regulações ou normas aplicáveis. Controles internos, por sua vez, vão além de conformidade com normas e regras, compreendendo a verificação para que os ativos e os recursos sejam utilizados em função dos propósitos da organização (*idem*, p.3-4), isto é, abrangendo também a eficiência e a eficácia operacional. Sendo assim, na visão de Miller, *compliance* é parte de controles internos, sendo que este último está ligado à função de conformidade interna em relação às normas e aos processos em prol da geração de valor para a firma.[7] Ele não fornece uma definição explícita para o gerenciamento de riscos.

Um guia frequentemente citado é o do Financial Reporting Council (FRC), gestor do The UK Corporate Governance Code. No guia específico sobre o assunto, o FRC considera que o gerenciamento de riscos e os controles internos sempre formarão um *pacote* integrado. Muito embora considere os controles internos como algo distinto do gerenciamento de riscos (FRC, 2014, p.8-9), essa distinção não é direta. O *compliance* seria apenas um dos objetivos de tal pacote. Ou, em suas palavras (*idem*, p.8):

> *The risk management and internal control systems encompass the policies, culture, organisation, behaviours, processes, systems and other aspects of a company that, taken together:*
>
> - *facilitate its effective and efficient operation by enabling it to assess current and emerging risks, respond appropriately to risks and significant control failures and to safeguard its assets;*

[7] No âmbito dos controles internos, Miller (*idem*, p.4-5) cita três "linhas de defesa" dentro da organização na asseguração dos controles definidos. A primeira corresponde às unidades operacionais e seus responsáveis diretos (em seu argumento, se estes forem bem sucedidos, não haveria violações); a segunda consiste em pessoas e divisões específicas de controle e monitoramento (Chief *Compliance* Officers, Chief Risk Officers); a terceira abrange a área de auditoria interna, que deve zelar pela conformidade das demais em última instância.
Na sequência, ele reconhece que tal estrutura é incompleta, uma vez que outros agentes (internos e externos) também estão envolvidos na asseguração de controles, tais como o conselho de administração (e seu comitê de auditoria), auditores externos, e, quando aplicável, órgãos governamentais. Num sentido mais amplo, acionistas ativistas, firmas de assessoria financeira (para acionistas), potenciais compradores hostis ("takeover bidders") e a imprensa também devem ser considerados, ao exercerem pressão em favor da construção de controles internos adequados.
Outro problema identificado pelo autor é o fato da segunda e a terceira linhas de defesa serem entidades de controle que são parte do próprio corpo de gestão, gerando um problema de circularidade sobre sua supervisão. Muito embora Miller tenha mencionado entidades externas que, de certa forma, exerçam pressão para que haja conformidade aos sistemas de gestão de risco e controles internos definidos, o mesmo não explora o assunto em profundidade.

- *help to reduce the likelihood and impact of poor judgement in decision-making; risk-taking that exceeds the levels agreed by the board; human error; or control processes being deliberately circumvented;*
- *help ensure the quality of internal and external reporting; and*
- *help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.*

O Committee of Sponsoring Organizations of the Treadway Commission (COSO) é bem mais claro na diferenciação. O gerenciamento de riscos trata da identificação, avaliação e administração de riscos diante de incertezas e da geração de valor. Além disso, o seu processo permite a administração de riscos de forma compatível com o apetite de risco da organização e **possibilita um nível razoável de garantia em relação à realização dos seus [organização] objetivos** (COSO, 2004, p.13). Por outro lado, controles internos têm a finalidade de "**possibilitar uma garantia razoável quanto à realização dos objetivos [da organização]**" (*idem*, p.109).

Dessa forma, explicitamente, o COSO considera controles internos como parte integrante do gerenciamento de riscos. É importante citar que a estrutura conceitual de gerenciamento de riscos do COSO foi uma adição à sua estrutura conceitual para controles internos (sem modificar a última), afirmando que os controles internos estão englobados e fazem parte integral do gerenciamento de riscos corporativos (*idem*, p. 109).

Ainda, para o COSO, pode existir uma estrutura conceitual de controles internos sem a estrutura de gerenciamento de riscos, dependendo dos objetivos que a organização deseja assegurar. Na estrutura isolada de controles internos, os objetivos a serem assegurados referem-se aos objetivos de garantir a eficiência e eficácia das operações, confiabilidade das demonstrações financeiras e compliance, enquanto que na estrutura de gerenciamento de riscos, há a adição de:

> "**another category of objectives, namely, strategic objectives,** which operate at a higher level than the others. Strategic objectives flow from an entity's mission or vision, and the operations, reporting, and compliance objectives should be aligned with them**.**" (*idem*, p.110, negrito nosso). [8]

Outra consideração importante na distinção é o escopo, sendo que a estrutura de gerenciamento de riscos corporativos amplia o componente de avaliação de riscos da estrutura de controle interno, criando quatro sub-componentes: fixação de objetivos[9] (que é comum à estrutura de controles internos, exceto pelos objetivos estratégicos), identificação de eventos que podem impactar os objetivos[10], avaliação de riscos e resposta a riscos" (*ibidem*).

A International Federation of Accountants (IFAC) também atrela o gerenciamento de riscos aos *objetivos* (IFAC, 2015, p.6), enfatizando que avaliações de risco deveriam ser feitas para questionar as premissas dos próprios objetivos quando ainda de sua formulação (p.11).

Em sua definição (p.6), o gerenciamento de riscos auxilia as organizações a tomar decisões informadas sobre os objetivos desejados; sobre o nível, natureza e magnitude de riscos que querem assumir na

[8] Bromiley *et al*. (2014, p.2) chegam a apontar correntes na literatura as quais, diferentemente do COSO, definem risco como algo objetivo e por si só existente, de forma independente dos objetivos definidos pela organização.
[9] Objetivos estratégicos, operacionais, de comunicação e de *compliance*, sendo os três últimos também existentes na estrutura de controles internos.
[10] Eventos que possam afetar os objetivos, de acordo com o framework do COSO, podem ser positivos ou negativos. Os positivos são tratados como oportunidades e os negativos como riscos.

persecução daqueles; e sobre os controles necessários para atingir tais objetivos. Ou seja, também para a IFAC, os controles são parte do processo de gerenciamento de riscos, e estão atrelados aos objetivos organizacionais.

Nessa revisão de literatura, é importante citar a definição de gerenciamento de riscos do ISO 31000 (ISO, 2009), padrões reconhecidos internacionalmente. Para eles, a estrutura [conceitual] de gerenciamento de riscos significa o *conjunto de componentes que fornecem as fundações (política, objetivos, mandato e comprometimento para administrar o risco) e os arranjos organizacionais (planos, relações, responsabilidades, recursos, processos e atividades) por desenhar, implementar, monitorar, revisar e melhorar continuamente as atividades coordenadas para direcionar e controlar uma organização no que refere a riscos*.

Não há um único ISO específico para controles internos, muito embora diversos deles abordem a questão de controle e *compliance*, como, por exemplo, as séries ISO 9000, ISO 14000 e ISO 27000. Dentro da estrutura de gerenciamento de riscos do ISO 31000, controle é visto como parte do processo de tratamento de riscos e inclui processos, política, mecanismos, práticas e outras ações tendo por objeto a alteração do risco. Nesse contexto, a natureza desse controle é diferente da dos controles internos, tanto de conformidade à regulamentação quanto de conformidade à eficiência dos processos operacionais.

De toda forma, Bromiley *et al*. (2014, p.7) lembram o caráter "*forward looking*" do gerenciamento de riscos, uma vez que o mesmo lida com resultados futuros incertos. Isso vai ao encontro de outras visões sobre o gerenciamento de riscos terem caráter único e distinto de controles internos ou *compliance*. Adicionalmente, Van der Elst (2013, p.28), ao buscar orientar a elaboração de diretrizes sobre o gerenciamento de riscos corporativos, destaca a separação dos objetivos operacionais e estratégicos dos objetivos de *compliance* e reporte financeiro. Para os primeiros objetivos, em sua visão, caberia ao conselho de administração definir um apetite organizacional pelo risco.

A noção de apetite pelo risco também implica na noção de tolerância ao risco. De acordo com o COSO (COSO, 2014, p.110), o apetite a riscos é a quantidade de risco estabelecida, de modo amplo, que uma empresa está disposta a aceitar na busca de sua missão/visão, enquanto a tolerância a risco é o nível aceitável de variação referente à realização dos objetivos.

É importante notar que os *frameworks* existentes, embora ajudem a entender a distinção entre gerenciamento de risco, controles internos e compliance, eles não passam sem críticas.

Power (2009) critica a adoção generalizada do gerenciamento de riscos (ou ERM - Enterprise Risk Management) que se ampara em estruturas conceituais que podem ser resumidas em a organização identificar os riscos materiais relativos a seus objetivos, desenhar os controles e as mitigações consistentes com uma medida de apetite pelo risco, e monitorar o processo inteiro, fazendo os ajustes necessários (p.849). O autor aponta que as raízes desse tipo de estrutura conceitual continuam sendo as noções de controle em contabilidade e auditoria.[11]

[11] Como base das críticas está o fato das organizações serem organismos complexos. Simplificadamente, as três principais questões (p.850) seriam: (i) a definição de um apetite pelo risco como processo organizacional pode ser problemático, uma vez que, para um mesmo evento, diversas áreas da organização possuem perspectivas diferentes (geralmente a ideia é a existência de uma métrica quantitativa); (ii) a lógica de que todo o processo descrito anteriormente, que envolve a organização inteira, deve ser auditável no conceito de auditoria financeira – de acordo com o autor, *em geral, a proliferação de normas internas sobre processos detalhados é assumida como uma falha de implementação, e ainda assim a premissa do modelo é a existência dessa proliferação* (para ser auditável no conceito de auditoria financeira), tornando o gerenciamento de riscos o *gerenciamento de tudo*,

Outra abordagem crítica vem de Lehuede, Kirkpatrick & Teichmann (2012, p.7). Eles chamam atenção para o fato de que o gerenciamento de riscos no contexto de governança corporativa não deve focar no aspecto técnico dos modelos de risco, mas sim em aspectos comportamentais. Em sua visão, um foco crucial seria em como as informações sobre a exposição organizacional ao risco são utilizadas dentro da organização, incluindo a sua transmissão para o conselho de administração. Para os autores, vários conselhos de administração (de empresas financeiras na crise financeira global de 2007/2008) não identificavam os riscos, não estavam conscientes das decisões estratégicas envolvidas e não tinham estruturado mecanismos de controle para supervisionar o apetite pelo risco, muito embora houvesse métricas de risco, como requisitos de capital (*idem*, p.8). Assim, uma das linhas de exploração dentro do contexto de governança seria a governança do gerenciamento de riscos dentro da empresa. [12]

Ainda que haja visões diferentes sobre gerenciamento de riscos, podemos concluir de forma resumida que:

- *Compliance* (aderência às normas e procedimentos definidos previamente) tende a ser visto na literatura como parte, seja de gerenciamento de riscos, seja apenas de controles internos, ambos com escopo mais amplo dentro da organização.
- A função de controles internos pode ser compreendida como tendo intersecção com um sistema de gerenciamento de riscos. O sistema de controles internos, além de *compliance*, busca assegurar que as operações da empresa sigam conforme o planejado, mitigando desvios, e, embora não questione aquilo que foi planejado, pode contribuir de forma crítica. Lembrando a definição de Miller no início dessa seção de que a função de controles internos compreende a verificação para que os ativos e os recursos sejam utilizados em função dos propósitos da organização (eficiência e eficácia operacional), podemos concluir que nem todas as atividades da função controles internos (operacional) endereçam "riscos" e nem todo controle de riscos relevantes pode ser tratados por meio da função controles internos.
- O gerenciamento de riscos é mais holístico, ao inserir-se não só nos contornos das operações, mas também no direcionamento estratégico da organização, incorporando diferentes perspectivas, tais como o ambiente externo e a reputação da organização. Também, gerenciamento de riscos é mais amplo, incluindo o processo de identificação, mensuração (qualitativa ou quantitativa), avaliação de riscos, bem como a definição da atitude da organização perante estes riscos e os seus tratamentos (inclusive controle).

Por fim, vale alertar para o fato de que, embora a palavra "riscos" possa ter uma conotação negativa[13] para muitas pessoas, a OCDE (Kirkpatrick, 2009, p.9) afirma que os reguladores devem compreender que o gerenciamento de riscos não requer que os riscos deixem de ser incorridos. A ideia é que os mesmos sejam compreendidos, gerenciados e, quando pertinente, comunicados.

Nessa linha, Enriques & Zetzsche (2013, p.13) diferenciam gerenciamento de riscos de mitigação de riscos. O gerenciamento de riscos inclui escolher entre (i) abster-se de incorrer no risco, (ii) impor medidas de controle preventivas e reativas para mitigar riscos operacionais, (iii) aceitar níveis de risco para atingir objetivos e (iv) transferir riscos, por exemplo, via hedge e seguro.

---

tendo como implicações custos operacionais elevados; (iii) por fim, apesar dos elevados custos devido à primazia da auditoria, o modelo *tem sido incapaz de articular e compreender os riscos críticos, particularmente aqueles associados à interconexão*.

[12] No conceito do COSO, o conselho de administração tem papel de supervisão, enquanto que no do ISO 31000 não há especificações.

[13] Estritamente falando, riscos podem ter consequências positivas ou negativas.

Kaplan & Mikes (2014, p.35) também argumentam no mesmo sentido, quando expõem sua tipologia de riscos. Os riscos podem ser (i) passíveis de prevenção (ou seja, indesejáveis sob todos os aspectos, sem benefícios estratégicos ao serem suportados) e controláveis via controles internos, auditoria interna e valores corporativos, porém sujeitos a uma relação de custo-benefício; (ii) riscos de execução de estratégia, para os quais as organizações podem buscar reduzir frequência e severidade de impacto via estratégias de identificação, mitigação e monitoramento; e (iii) riscos externos incontroláveis, para os quais a organização poderia se preparar e reduzir impactos via exercícios de análise de cenário, planejamento de contingências e transferência de riscos. [14]

Nesse sentido, um bom gerenciamento de riscos pode, inclusive, implicar a *elevação* do grau de risco incorrido por uma organização em busca de seus objetivos (e, por consequência, de retorno).

2.1.2. Gerenciamento integrado de riscos

Um dos desdobramentos da visão estratégica do gerenciamento de riscos consiste no debate sobre a responsabilidade das instâncias organizacionais pela sua formulação, definição e/ou aprovação. O gerenciamento pode ocorrer de forma autônoma nas diversas áreas/departamentos/unidades organizacionais, em que cada uma delas considera seus próprios objetivos e parâmetros (modelo de silos fechados), ou então de forma integrada, havendo coordenação de visão dentro da organização.

O assunto é tratado extensivamente na literatura e a tendência tem sido pela integração, conforme pode ser visto nos exemplos abaixo.

Lehuede, Kirkpatrick & Teichmann (2012, p.8) citam como um dos problemas de governança evidenciados pela crise financeira de 2008 o gerenciamento de riscos por unidade ou divisão organizacional (modelo de silos fechados), ao invés de uma gestão com base na organização como um todo.[15] Tricker (2015, p.200) aponta que, nesse tipo sistema de "silos fechados", as responsabilidades são delegadas às médias gerências, cujo foco é mitigar seus próprios erros e ameaças operacionais.

Por sua vez, a IFAC (2015, p.10) pontua que a maturidade do processo de gerenciamento de riscos progride conforme ele move do modelo de silos em direção a incluir controles internos e gerenciamento de riscos como parte natural e integral do sistema de gerenciamento organizacional. Dessa forma, para a IFAC (*idem*, p.12-13), a função de uma área de gerenciamento de riscos corporativos seria a de ser uma facilitadora de processos a nível organizacional (uma função de liderança e coordenação de projetos interdisciplinares), custodiante de *frameworks* (função de consultoria e inteligência interna) e uma certificadora de eficácia do gerenciamento de riscos de cada área (processos de monitoramento).

Nessa linha, Itner & Keusch (2015, p.12-13) destacam os benefícios do gerenciamento de riscos organizacionalmente integrado, também nomeado muitas vezes de ERM (Enterprise Risk Management). Dentre eles, melhor compreensão dos riscos gerais da empresa, de seus fatores causais e das interdependências de risco dentro da organização. Isto permitiria uma visão de portfólio, no qual

[14] Essa classificação possui paralelos com a de Tricker (2015, p.197 e p.200), que inclui riscos operacionais (ameaças internas emanando de própria organização, tais como incêndios), riscos gerenciais (riscos das atividades operacionais) e riscos estratégicos, que incluem ameaças externas à organização.

[15] Os mesmos (*idem*, p.6) ainda mencionam sistemas assimétricos de remuneração que incentivaram a tomada excessiva de riscos pelas empresas do setor financeiro. Bromiley *et al*. (2014, p.8) mencionam o papel dos bônus concedidos por divisão corporativa, fator que pode prejudicar a implementação de ERM – Enterprise Risk Management e a da maximização do valor da firma.

a organização pode explorar correlações para coordenar a tomada de risco e a resposta a ele, de forma a minimizar a volatilidade e riscos de cauda.

Bertinetti, Cavezzali & Gardenal (2013, p.5-6), numa revisão bibliográfica, cita os mesmos benefícios, com a adição da redução de duplicidade de despesas das diversas áreas/unidades. Entre outras constatações de sua revisão, tem-se aquela das empresas maiores (financeiro), mais diversificadas geograficamente, com maior grau de alavancagem e base acionária institucional serem mais propensas a adotar o ERM.

Os mesmos autores ainda citam (*idem*, p.2) que a pressão para a adoção de um novo modelo de gerenciamento de riscos não se limitou aos reguladores, abarcando firmas de consultoria, agências de rating e pesquisadores acadêmicos. Em relação a agências de rating, os autores notam que a S&P assinala um rating de ERM em sua análise de rating geral para seguradoras. Esse rating de ERM leva em conta 5 categorias, e as escalas aumentam conforme o nível ao qual o processo de gerenciamento de riscos aproxima-se de ERM.

Ao analisarmos os critérios da Standard & Poors (Standard & Poors, 2013), identificamos as seguintes categorias: a primeira é o desenvolvimento de uma cultura de gerenciamento de riscos (incluindo evidências do envolvimento do conselho de administração no programa de ERM e a documentação da estrutura organizacional do ERM); a segunda é a existência de controles de risco (como políticas formais, monitoramentos e revisões externas); a terceira são evidências de processos concretos de gerenciamento de riscos; a quarta são evidências de modelos de risco; e a quinta, finalmente, consiste em evidências do gerenciamento estratégico de risco.

De uma forma geral, ao envolver a estratégia das organizações e as interações entre as diversas áreas, é consequência natural supor que o gerenciamento de riscos requer uma formulação a nível organizacional, não apenas sub-organizacional, muito embora a execução dos processos ocorra em todos os níveis.

2.2. Integração do gerenciamento de riscos nos conselhos de administração

Outro enfoque sobre a formulação e definição do direcionamento geral de gerenciamento de riscos diz respeito a duas questões necessariamente interligadas: quais órgãos dentro da organização deveriam ter essa responsabilidade e qual o escopo da responsabilidade desses órgãos. Destaca-se que, neste relatório, o termo gerenciamento de riscos é utilizado em geral para referir à sua formulação ou à sua estrutura geral. Quando se desejou falar da execução de gerenciamento de riscos, o sentido foi deixado claro.

2.2.1. Atribuição de responsabilidades

Em auxílio à resposta da primeira questão, ao compreender o gerenciamento de riscos como essencial para atingir os objetivos da organização, inclusive os estratégicos, torna-se razoável atribuir essa responsabilidade ao órgão responsável pelo direcionamento da empresa e pelas decisões estratégicas.

A IFAC (2015, p.12) argumenta nesta linha, dizendo que a responsabilidade pelo gerenciamento de riscos deve caber aos responsáveis a definir os objetivos organizacionais. Ao mesmo tempo, Tricker (2015, p.170), ao discutir as funções do conselho de administração, afirma que *um dos deveres primários do conselho é garantir que a empresa esteja indo na direção correta* e que *a formulação estratégica é o processo de gerar e rever os direcionamentos alternativos de longo prazo que levem a*

companhia à realização de seus propósitos, consistente com o perfil de risco aceitável para ele.[16] Esta ainda é a recomendação mais recente da OCDE em seus princípios de governança corporativa.[17]

Itner & Keusch (2015, p.15-16), ao revisarem a bibliografia sobre envolvimento dos conselhos em gerenciamento de riscos, definem quatro níveis possíveis de envolvimento do conselho no gerenciamento de riscos: (i) o conselho *não* se envolve de forma alguma com o gerenciamento de riscos; (ii) ele se envolve como um todo; (iii) ele se envolve apenas via um de seus comitês; e (iv) se envolve via ambos, um comitê específico e o conselho como um todo.[18]

No estudo, os autores (*idem*, p.10-11) também discutem os prós e contras da utilização de comitês específicos versus o conselho todo. Dentre os problemas envolvendo a utilização exclusiva de comitês de conselho, eles citam a subutilização da diversidade dos recursos humanos do conselho, a incapacidade de supervisão geral da companhia por um único comitê e a confusão gerencial advinda da sobreposição de trabalhos dos diversos comitês de conselho. Por outro lado, em prol do uso de comitês específicos, estariam vantagens de maior foco, especialização e interação com especialistas, centralização da supervisão, caminhos definidos para fluxo de informação de risco dentro da organização e o papel simbólico de um comitê de riscos.[19]

2.2.2. Escopo das responsabilidades

Conforme citado e discutido adiante, os princípios mais recentes de governança corporativa da OCDE conferem responsabilidades finais de desenho, supervisão e monitoramento dos sistemas de gerenciamento de riscos corporativos aos conselhos de administração e seus comitês.

Nesse sentido, também vale a pena sistematizar o guia do FRC (Council, 2014, p.5) em seis pontos principais de responsabilidades do conselho de administração no tocante ao gerenciamento de riscos: (i) *implementação de sistemas* de gerenciamento de risco e controles internos; (ii) *avaliação de riscos* e *determinação do apetite pelo risco*; (iii) *gerenciamento dos principais riscos*[20]; (iv) *monitoramento dos sistemas* de gestão de risco e controles internos e do trabalho dos gestores[21]; (v) a *transmissão* dentro da organização *do apetite pelo risco* via cultura e mecanismos de remuneração; (vi) *assegurar comunicação* interna e externa adequada sobre gerenciamento de riscos e controles internos.[22]

A estrutura proposta pelo FRC possui alguma similaridade com a proposta pelo COSO, esta possuindo oito etapas (COSO, 2014, p.22), muito embora o COSO atribua papel basicamente de supervisão ao

[16] Tricker afirma também que o papel do conselho na formulação estratégica vai depender muito das características da empresa. Até mesmo pelo tempo disponível, é possível o arranjo onde os executivos tenham papel fundamental na revisão e elaboração de propostas, que são submetidas ao conselho para discussão e eventual reformulação, antes da aprovação pelo conselho.

[17] Ver discussão na página 22.

[18] A OCDE (2014, p.18) afirma que, de acordo com suas pesquisas, os comitês de auditoria tendem a focar demasiadamente em controles internos para fins de reporte financeiro, divorciando-se da parte estratégica.

[19] O Financial Stability Board, por sua vez, considera como boa prática a existência um comitê específico de risco (ou seja, diferente do comitê de auditoria), presidido por um membro independente do conselho (OCDE, 2014, p.17).

[20] De acordo com o guidance (p.8), "principal risks" são riscos que "given the company's current position, could threaten the company's business model, future performance, solvency or liquidity, irrespective of how they are classified or from where they arise".

[21] De acordo com o guidance (p.5), a execução das políticas de gerenciamento de risco definidas pelo conselho de administração cabe ao corpo gestor. Contudo, "the board needs to satisfy itself that management has understood the risks, implemented and monitored appropriate policies and controls, and are providing the board with timely information so that it can discharge its own responsibilities".

[22] A comunicação interna inclui uma política de *whistleblowing* (p.9).

conselho. A primeira seria a definição de um ambiente interno, com o estabelecimento de uma filosofia quanto ao tratamento de riscos e o limite ao apetite pelo risco. Partindo disso, definem-se os objetivos organizacionais (estratégicos, operacionais, de comunicação e compliance) e caminha-se para a identificação de eventos capazes de impactá-los. Identificados os eventos, avaliam-se os riscos, define-se uma resposta aos mesmos e parte-se para as atividades de controle, comunicação (interna e externa) e monitoramento. No entanto, o COSO, conforme já mencionado anteriormente, conduz a modelos técnicos, enquanto que FRC abre espaço para a determinação de aspectos de governança.

Por fim, Tricker (2015, p.206) apresenta uma matriz, abaixo, com a estrutura conceitual das responsabilidades do conselho de administração no gerenciamento de riscos, considerando a dimensão "ambiente interno ou externo" e o foco, se "presente/passado ou futuro".

Tabela 1 - Estrutura conceitual das responsabilidades no gerenciamento de riscos

	Interno	Externo
Presente/Passado	Monitoramento e supervisão de risco	Prestação de contas sobre gerenciamento de riscos a acionistas, reguladores, e outras partes interessadas
Futuro	Formulação de políticas de riscos	Reconhecimento, análise e avaliação de risco estratégico

2.3. Pesquisas empíricas e geração de valor

As pesquisas empíricas sobre o gerenciamento de riscos pertencem a diversos campos de estudo. Algumas das pesquisas são mais gerais e versam sobre a relação entre a estrutura organizacional de gerenciamento de riscos e seus impactos sobre as métricas de risco. Outras são mais específicas e lidam apenas com a eficácia de alguns mecanismos de gerenciamento de riscos financeiros.

Em estudo recente, Itner & Keusch (2015, p.4; p.7-8) hipotetizam que a forma de estruturação dos conselhos quanto à responsabilidade no gerenciamento de riscos teria apenas uma relação indireta com a eficácia da redução do risco corporativo.

Em seu raciocínio, a forma de estruturação do conselho na sua responsabilidade pelo gerenciamento de riscos (conselho como um todo, via comitês, ou ambos) impactaria o nível de envolvimento do conselho com atividades de gerenciamento de riscos.[23] *O nível de envolvimento do conselho, por sua vez, levaria a maior grau de maturidade dos processos de gerenciamento de risco, o que finalmente reduziria o risco corporativo*.

[23] Os autores (*idem*, p.13) sugerem que tanto a forma da estruturação quanto o envolvimento do conselho podem ter uma ligação direta na redução de riscos e testam as duas variáveis simultaneamente.

Nesse sentido, os autores buscam avaliar quatro hipóteses: (i) o envolvimento do conselho com o gerenciamento de riscos teria grau máximo quando as responsabilidades são designadas ao conselho como um todo (p.10); (ii) a presença de um comitê específico de risco estaria positivamente associada ao envolvimento do conselho com o gerenciamento de riscos (p.11); (iii) maior envolvimento do conselho com o gerenciamento de riscos estaria positivamente associado com à maturidade dos processos de gestão de risco da empresa (p.12); e (iv) a maturidade dos processos de gestão de risco da empresa estaria negativamente associada a medidas de risco como volatilidade e risco de cauda (*tail risk*).

As possíveis formas de estruturação são aquelas já mencionadas anteriormente: o conselho como um todo, apenas via comitê específico, via ambos, ou nenhum deles (ou seja, não há responsabilidade por parte do conselho). Já o envolvimento do conselho com o gerenciamento de riscos é medido através de quatro variáveis: a compreensão do conselho ("*board understanding*", p.16), os reportes do conselho ("*board reporting*", p.16-17), o alinhamento do conselho ("*board alignment*", p.17) e a comunicação do conselho sobre gerenciamento de riscos ("*board and risk management communication*", p.18). [24]

O grau da maturidade dos processos de gestão de risco corporativo, por sua vez, é dado por um índice da seguradora AON, que leva em conta dez fatores, dentre os quais se incluem a compreensão e o comprometimento do conselho com o gerenciamento de riscos, a supervisão do conselho sobre o corpo gestor, a participação dos *stakeholders* no processo de gerenciamento de riscos, a integração entre o gerenciamento de riscos e os processos de capital humano, questões relacionadas a informações e comunicação de riscos, além da quantificação e compreensão de riscos (p.18-19).

Por fim, as medidas de risco consideradas (p.20-21) são a volatilidade das ações (desvio padrão de retornos diários), o risco idiossincrático (desvio padrão dos resíduos de um modelo estatístico baseado no CAPM - "*market model*") e uma *proxy* para o risco de cauda (negativo da média dos retornos dos 5% piores dias de retorno da ação).

Adicionalmente, variáveis de controle (tanto de governança corporativa como financeiras e gerais) foram incluídas nos testes para segregar efeitos externos sobre o gerenciamento de riscos (p.21-23).

Dentre os resultados (p.24-25), podemos mencionar que a análise de correlações entre a estruturação do conselho e o envolvimento do conselho mostra relação negativa quando não há nenhuma responsabilidade quanto aos membros do conselho ou quando apenas um comitê do conselho tem responsabilidade; e relação positiva e estatisticamente significativa quando a responsabilidade ocorre no conselho como um todo, bem como quando ocorre a responsabilidade em conjunto do conselho como um todo e do comitê do conselho (p.25-26).

Os resultados também apontam para a irrelevância estatística dos requerimentos da NYSE para que o comitê de auditoria se envolva com o gerenciamento de riscos, uma vez que as empresas listadas na NYSE não apresentaram envolvimento do conselho estatisticamente maior que as demais (p.27-28).

Além da forma de estruturação do conselho na sua responsabilidade, algumas das variáveis de controle apresentam significância estatística sobre o envolvimento do conselho com o gerenciamento de riscos. Dentre as variáveis com relação positiva citam-se a qualidade do *disclosure* financeiro da companhia[25], o número de diretores independentes, a existência de um presidente independente do

[24] As variáveis são calculadas com base em respostas dadas entre 2011 e 2013 para uma pesquisa internacional da seguradora AON com empresas listadas em bolsas (p.13-14 e Apêndice A).

[25] Litov & Yeung (2008), ao analisarem empiricamente a relação entre grau de proteção ao investidor e a tomada de riscos pelas empresas (amostra de 1992 a 2002 com empresas de 39 países), encontram correlação positiva entre a qualidade do *disclosure* financeiro e a tomada de riscos pelas empresas (p.26; p.28).

conselho de administração e alavancagem financeira. Enquanto isso, a educação financeira dos membros do conselho (fração dos membros com educação formal voltada para finanças) e o caixa disponível apresentaram relação negativa (p.28-29).

Em relação à hipótese sobre a maturidade dos processos de gestão de risco, o estudo mostra que ela está apenas diretamente relacionada ao grau de envolvimento do conselho com o gerenciamento de riscos (p.30). Poucas variáveis de controle são significativas ao explicar a maturidade dos processos de gestão de risco, com destaque para o tamanho da firma, positivamente relacionada (p.31) .[26]

Para os autores, a análise empírica confirma, portanto, a proposição inicial de que as formas de responsabilização do conselho pelo gerenciamento de riscos não impactam as métricas de risco diretamente, apenas indiretamente. Ou seja, corrobora-se a terceira e quarta hipóteses – um maior envolvimento do conselho está positivamente associado com a maturidade dos processos de gestão de risco da empresa e essa maturidade, por sua vez, está negativamente relacionada com as métricas de risco (p.32).

Além disso, os resultados do estudo mostram que algumas variáveis de controle também são significativas na redução das métricas de risco, tais como menos conselheiros sobrecarregados e um número absoluto maior de conselheiros independentes (muito embora uma maior *fração* de independentes eleve as métricas de risco na modelagem) (p.33).

Outra relação constatada (p.35-36) é a de que a atribuição de responsabilidades ao conselho como um todo e o decorrente maior nível de envolvimento do conselho não tornam as empresas demasiadamente avessas ao risco, reduzindo seus retornos. As responsabilidades ao nível do conselho como um todo, inclusive, elevam os retornos das empresas.

Por fim, empresas que experimentaram um evento significativo de risco nos dois anos anteriores continuaram com métricas de risco mais elevadas que as de seus pares, ainda que com indicadores de envolvimento do conselho nos mesmos patamares. Isto, associado à constatação de menor grau de maturidade dos processos de gerenciamento de riscos nessas empresas, indicaria que o ato de atribuir responsabilidades ao conselho de administração teria sido um ato mais simbólico em meio à pressão do que um ato efetivo para o gerenciamento de riscos (p.33).

Outro campo de pesquisa pode ser ilustrado pelo trabalho de Bertinetti, Cavezzali & Gardenal (2013, p.6), que analisa a agregação de valor em função da implementação do ERM, utilizando dados de 200 companhias europeias, entre os anos 2002/2011.

Em seu trabalho, os mesmos referenciam (p.4) alguns estudos empíricos anteriores cuja conclusão foi de que a implementação do ERM trouxe ganhos às empresas na forma de resultados e preços de ativos menos voláteis, aumentos de eficiência no uso do capital, maiores sinergias entre diversas atividades de gerenciamento de risco, e maior consciência da importância do último dentro da organização.

O paper (p.17) utiliza dados de relatórios financeiros e indícios da existência de um programa de ERM, criando uma variável *dummy* para cada observação (ao final do período, foi verificado que 61% da amostra adotava ERM, enquanto que, no início do período, apenas 3,5% da amostra adotava-o). A pesquisa testa a hipótese de o ERM ter agregado valor às empresas durante o período do estudo, além de ter por objetivo a identificação dos determinantes da adoção do ERM.

[26] Litov & Yeung (2008, p.31-32), também notam em sua amostra que firmas maiores tendem a possuir menores métricas de risco.

Para a primeira hipótese, a *proxy* do valor da firma é uma estimativa do Q de Tobin (p.8). As variáveis de controle para o teste incluem o logaritmo natural do tamanho da firma, a alavancagem financeira, o crescimento das vendas, o retorno sobre os ativos, o pagamento de dividendos e o beta. Os resultados do estudo mostram que a adoção de ERM impactou positivamente o Q de Tobin para as empresas consideradas na amostra, independentemente do setor (p.10-11), muito embora mereça ser destacado o baixo coeficiente de determinação (= 0,12) da regressão (p.17).

Já em relação aos determinantes (p.9), são incluídas novamente variáveis de controle como o tamanho da firma (espera-se relação positiva entre adoção do ERM e tamanho da firma) e a alavancagem financeira (pesquisas empíricas mostram relação ambígua, ora incentivando, ora desincentivando a adoção do ERM).

Além dessas variáveis de controle, é considerada também a "opacidade" (proporção de ativos intangíveis, fator que se espera incentivar a adoção do ERM), a proporção de ativos de alta liquidez ("financial slack", sobre o qual não haveria evidência empírica unânime) e a variação anual do EBIT e do valor da firma. Como conclusão apontada pelos autores, pode-se destacar a significância estatística da opacidade, do tamanho da firma e da proporção de ativos de alta liquidez como fatores que facilitam a adoção do ERM pelas empresas (p.11).

Ainda quanto aos efeitos da adoção de ERM, alguns estudos citados por Mikes & Kaplan (2014, p.6), tentam explicar a adoção do ERM. Em um primeiro bloco de estudos, considera-se que há adoção do ERM quando há contratação de um CROs ou registros de influência do conselho de administração e executivos pró-adoção do ERM. Dois desses estudos encontram correlação positiva entre a adoção do ERM e redução do nível de volatilidade dos fluxos de caixa.

Outro bloco de estudos citados (p.8) tendo como objetivo auferir a geração de um prêmio de valor nas ações devido à adoção do ERM utiliza como *proxies* de tal adoção anúncios corporativos da adoção de um programa de ERM, anúncios de contratação de um CRO e alguns índices de adoção do ERM calculados por agências de *rating*. Aqui, os resultados empíricos são mistos.

No que diz respeito ao gerenciamento de riscos financeiros, a abordagem *mainstream* de finanças sempre questionou a necessidade de um programa de gerenciamento corporativo de riscos, uma vez o investidor final se importaria apenas com o risco sistemático (beta), ou seja, aquele não diversificável.[27] Mesmo assim, além de estudos mais gerais do tipo daqueles citados acima, há diversos trabalhos empíricos sobre a geração de valor pelo processo de gerenciamento de riscos financeiros, objetivando argumentar que as empresas devem reduzir a exposição ao risco quando não possuem vantagens comparativas e vice-versa (Bromiley *et al*., 2014, p.3).

Monda, Giorgino & Mondolin (2013, p.4-5) salientam quatro razões possíveis para que o gerenciamento de riscos corporativos possa ser uma forma de geração de valor para a firma, *ainda que foquem apenas em operações de hedge financeiro*. A primeira seria a redução de custos de transação, especialmente no caso de bancarrota, ao reduzir as probabilidades de default (*idem*, p.17-18). A segunda consistiria na coordenação das políticas de financiamento e investimento, reduzindo o custo

[27] Monda, Giorgino & Mondolin (2013, p.2) mostram que o gerenciamento de riscos corporativos como atividade capaz de gerar valor vão de encontro aos teoremas de Modigliani & Miller. Atividades de hedge, de acordo com os modelos CAPM, poderiam até reduzir valor da firma (*idem*, p.4). Contudo, os mesmos apontam que o gerenciamento de riscos corporativos via hedge financeiro pode agir como um substituto imperfeito do *disclosure* de informações (*idem*, p.22), pois os gestores das empresas seriam capazes de mitigar alguns riscos com informações melhores do que as informações passíveis de serem detidas pelo investidor final.

de capital.[28] A terceira corresponderia à redução de tributos[29] e a quarta seria a mitigação de conflitos de agência (acionistas x detentores de dívida e acionistas x gestores). [30]

Por outro lado, os autores em seu trabalho afirmam (*ibidem*) que estudos sobre o gerenciamento de risco tradicional (focados na realização de hedge e seguros) possuem resultados controversos, com algumas pesquisas mostrando que há geração de valor e outras que não há, devido ao baixo valor relativo das posições de derivativos no setor não financeiro.

Smithson & Simkins (2005), focando no gerenciamento de riscos financeiros, fazem um apanhado geral dos trabalhos empíricos existentes até 2005, com o objetivo de responder quatro questões (p.8): (i) se os riscos financeiros se refletem nos preços dos ativos; (ii) se o uso de derivativos está associado à redução destes riscos; (iii) se há relação entre a volatilidade dos fluxos de caixa e o valor da firma; e (iv) se há relação entre o uso de técnicas de gerenciamento de risco financeiro e o valor da firma.

No que tange à primeira pergunta (p.10-12), os mesmos examinam 21 trabalhos empíricos, concluindo que há impacto no caso de empresas do setor financeiro (nove trabalhos). No que diz respeito às empresas não financeiras, 11 de 12 estudos abordam o risco cambial, com os autores afirmando que poucas empresas apresentaram variação estatisticamente significativa de seus retornos em função dos movimentos cambiais. É fato que o risco cambial está negativamente relacionado ao grau de hedge operacional ("operational hedging") das empresas. Muitas vezes é menor para firmas maiores, que tendem a ser multinacionais e disporem de hedge natural.

Para responder a segunda pergunta (p.12), os autores examinam 15 estudos, dos quais seis focam em instituições financeiras. As empresas financeiras teriam risco mitigado pelo uso de derivativos, enquanto oito dos nove estudos sobre as empresas não financeiras concluíram que o uso de derivativos cambiais reduziu a sensitividade dos retornos das ações ao fator de risco cambial (volatilidade).

No que diz respeito à terceira pergunta (p.13), os autores analisam três estudos, sendo que um desses relacionou a volatilidade do fluxo de caixa a uma queda nos investimentos, enquanto outros dois encontraram uma relação negativa entre volatilidade dos fluxos de caixa e dos resultados e o valor da firma.

Por fim, para responder a pergunta final (p.14-15), os autores analisam dez estudos, sendo que o mais recente é de 2001. Para auferir o valor da firma, nove dos dez estudos utilizaram o Q de Tobin como *proxy*. Um dos estudos referia-se a instituições financeiras, cinco eram sobre corporações industriais e os demais quatro sobre usuários e produtores de commodities.

---

[28] Os mesmos (i*dem*, p.23) consideram que uma redução na volatilidade dos fluxos de caixa poderia evitar um descasamento entre o cronograma de investimentos e a captação planejada de recursos, descasamento esse que poderia inesperadamente encarecer e paralisar projetos com VPL *ex-ante* positivo.

[29] Há uma suposição (*idem*, p. 26) de que uma menor volatilidade dos fluxos de caixa poderia gerar uma capacidade extra de alavancagem via custos mais baixos. Supõem ainda que o risco financeiro adicional seria compensado pelas vantagens tributárias do uso do capital de terceiros. Ainda consideram que uma menor volatilidade dos fluxos de caixa poderia auxiliar o planejamento tributário, muito embora não encontrem muito respaldo em pesquisas empíricas (*idem*, p. 28).

[30] Uma das razões especificadas por Monda, Giorgino & Mondolin (*idem*, p.7-8) é o risco de investimento em projetos de altíssimo risco quando a empresa se encontra em situação de estresse financeiro, situação na qual os acionistas buscam recuperar o valor da firma à custa dos detentores de dívida, tendo pouco a perder. A gestão de riscos minimizaria a volatilidade dos fluxos de caixa e do valor da firma, reduzindo as chances desse patamar extremo ser atingido (p.9). Outro conflito de interesses apontado (p.12-13) é de os gestores estarem mais expostos a risco específico do que os acionistas, o que poderia levá-los a serem demasiadamente conservadores ao conduzir a organização. Isto, por sua vez, poderia ocasionar problemas como a diversificação de investimentos corporativos para além das competências da organização. O gerenciamento de riscos corporativos poderia então mitigar tal problema.

O estudo sobre o setor financeiro correlacionou o uso de derivativos de juros e câmbio a maiores valores de firma. Os cinco estudos sobre corporações industriais apontaram em favor de uma relação positiva entre o uso de derivativos de câmbio e o valor da firma. Um estudo sobre companhias aéreas (usuárias de commodities) concluiu positivamente em favor do gerenciamento de riscos financeiros. Contudo, três estudos sobre produtores de commodities (óleo e gás e ouro) concluíram que as técnicas de gerenciamento de riscos financeiros não possuíam efeitos positivos sobre o valor da firma.

Em conclusão, podemos dizer que há justificativas teóricas para a adoção do gerenciamento de riscos corporativos em termos de geração de valor (incluso gerenciamento de riscos financeiros), bem como evidências empíricas. No entanto, conforme apresentado acima, não há unanimidade nos resultados empíricos, constatação para a qual devemos levar em conta as limitações dos métodos quantitativos nas ciências sociais e a dificuldade de mensuração das variáveis de gerenciamento de riscos.

3. Panorama internacional – normatização e práticas

3.1. Normatização vigente

Apesar da concepção de gerenciamento de riscos estar relacionada com governança corporativa ser relativamente recente, conforme afirmado na introdução deste trabalho, já podem ser encontrados diversos dispositivos em outras jurisdições, sejam regulamentações sejam códigos de governança *comply or explain*.

No intuito de facilitar a compreensão da leitura, sem a necessidade de abordar detalhes que não são foco deste trabalho, **tanto leis, regulamentações ou códigos de governança *comply or explain* serão tratados simplificadamente como "normatização/regulamentação" em todo o nosso trabalho**.

De fato, em um levantamento conduzido pelo Grupo Interagentes[31], que está promovendo a elaboração do Código Brasileiro de Governança Corporativa, dos 21 países analisados, a adoção dos códigos de governança *comply or explain* é obrigatória para as empresas listadas em bolsa em 16 deles, por meio de legislação ou normativo dos reguladores, ainda que, em vários casos, tenham atribuído às bolsas o dever de tornar a adoção dos códigos obrigatória. [32]

3.1.1. Formas e aspectos gerais das diretrizes

Para balizar o panorama normativo existente, exemplificado a seguir, pode ser útil ter em mente a tipificação utilizada por Enriques & Zetsche (2013, p.3-4). Ao comentarem o que chamam de "juridification" [33] do gerenciamento de riscos, os autores apresentam seis formas básicas de normatização imposta:

- requerimentos genéricos para que haja adoção de práticas de gerenciamento de riscos (sem prescrever quais são as práticas);
- prescrição de determinadas práticas *específicas* de gerenciamento de riscos;
- prescrição de arranjos de específicos de governança corporativa (determinando responsabilidades e atribuições para determinados órgãos da empresa);
- validação de modelos de gerenciamento de riscos em troca de regulamentação mais favorável (em seu exemplo, a possibilidade de menores requerimentos de capital para bancos com modelos internos de *rating*, conforme previsto nas regras de Basiléia II e III);
- imposição para gestores de deveres de monitoramento do gerenciamento de riscos; e
- requerimentos para que haja *disclosure* sobre o gerenciamento de riscos corporativos.

Os mesmos (p.5-6) ainda distinguem um fenômeno normatizador mais amplo, o de "process-based" ou então "management-based regulation", no qual ao invés de prescrever comportamentos e objetivos definidos, os reguladores buscam exigir que as empresas desenvolvam planejamento interno e práticas gerenciais, conferindo maior flexibilidade para as empresas no cumprimento de exigências.

[31] O Grupo Interagentes é formado por 11 entidades (ANBIMA, ABRAPP, ABRASCA, ABVCAP, AMEC, APIMEC, BMF&BOVESPA, BRAiN, IBGC, INSTITUTO IBMEC e IBRI), além de ter a CVM e o BNDES como membros observadores. O Código Brasileiro de Governança Corporativa está sendo elaborado no formato "Pratique ou Explique" e há intenção de que a sua adoção seja obrigatória, ao menos, para as empresas com ações negociadas em bolsa.

[32] Países em que adoção não era de alguma forma mandatória ou que as recomendações já tinham sido significativamente incorporadas pela regulamentação: Índia, México, Rússia, Taiwan, Turquia.

[33] "…what we call the juridification of risk management (hereinafter also RMJ), i.e. the fact that risk management arrangements become legally relevant" (p.3-4).

3.1.2. Exemplos de normatização

A. OCDE

De acordo com OECD Principles on Corporate Governance (2015)[34], entre as funções chaves do conselho está a de revisar e direcionar as políticas e os procedimentos de gerenciamento de riscos (OCDE, 2015, p. 53). O Princípio VI, seção D1, acrescenta ainda que uma área de importância crescente nas funções do conselho é a supervisão do gerenciamento de riscos na empresa, envolvendo a prestação de contas e as responsabilidades pela administração de riscos e especificando o grau de risco aceito pela empresa frente aos objetivos e como esta irá gerenciar os riscos inerentes a suas operações e relações (p.53-54). [35] Diz ainda que um direcionamento para o corpo executivo (que administra os riscos) é crucial para que este possa trabalhar dentro do perfil de risco desejado.

Cabe ainda ao conselho[36] assegurar a integridade dos sistemas contábeis e de reporte financeiro e que haja sistemas de controles internos adequados, em particular para gerenciamento de riscos, controles financeiros e operacionais (p.56) e *compliance*. Afirma também que seu comitê de auditoria deve monitorar a eficácia e a integridade do sistema de controles internos (p.59). Considera-se adicionalmente que, dependendo do tamanho da empresa e seu perfil de risco, deve ser considerada a instalação de um comitê especializado em gerenciamento de riscos (*ibidem*).

É importante notar a importância de comunicação nos princípios: por um lado o Princípio V, seção A7, afirma que a empresa deve divulgar os riscos relevantes e previsíveis e considera como boa prática o *disclosure* dos sistemas utilizados para monitorar e gerenciar riscos (p.46). Por outro lado, o Principio VI, seção F, destaca a importância de o conselho assegurar o seu acesso a informações acuradas, relevantes e tempestivas para que possa desempenhar as suas funções apropriadamente.

Vale ressaltar que os princípios até então vigentes (OCDE, 2004) seguiam linha muito próxima, sem, no entanto, enfatizar o papel de liderança do conselho no monitoramento. Outra diferença relevante era a ausência da recomendação para que os comitês de auditoria monitorassem a eficácia e a integridade do sistema de controles internos e a ausência da recomendação para que os conselhos considerem a relevância de um comitê específico de riscos.

B. EUA

Van der Elst (2013, p.2-3) lembra que nos EUA, dada a liberdade conferida pelas leis societárias para a implementação das políticas de governança dentro do sistema de "*common law*", as responsabilidades dos conselheiros sobre o gerenciamento de riscos são avaliadas *ex-post* em decisões judiciárias. No caso americano, decisões judiciais sobre o assunto atrelam esta responsabilidade dos conselheiros a seu dever mais geral de diligência.

Itner & Keusch (2015, p.6) consideram que, nos EUA, a NYSE por meio de suas regras de listagem requer que os comitês de auditoria discutam as diretrizes e políticas que governam a avaliação e o

[34] Em 2015, foi aprovada a versão revisada de OECD Principles of Corporate Governance. Os Princípios foram divulgados em 1999, tendo sido revisados em 2004.
[35] O relatório da OCDE (2014, p.16) sobre gerenciamento de riscos afirma que a normatização nos países submetidos à revisão [no âmbito daquele trabalho] tendia a não focar nos sistemas de gerenciamento de risco propriamente ditos, nem na compatibilidade entre os sistemas e o apetite ao risco. Também não há nos Princípios da OCDE maior nível de detalhamento, porém, deve-se lembrar que princípios são, por natureza, *high level*.
[36] Princípio VI, D7.

gerenciamento de riscos. A SEC, por sua vez, requer que a maioria das empresas publicamente negociadas divulgue o papel desempenhado pelo conselho de administração na supervisão dos riscos. Bertinetti, Cavezzali & Gardenal (2013, p.2) ainda nos lembram do recente requisito no âmbito do TARP [37] para que as empresas financeiras certifiquem que seus pacotes de remuneração não incentivem a organização tomar riscos considerados excessivos. [38]

C. Europa

Van der Elst (2013, p.7-10) mostra que, na União Europeia, novas diretrizes de regulamentação requisitaram em 2004 que os relatórios anuais e periódicos das empresas incluíssem uma descrição dos principais riscos e das incertezas com as quais as empresas se deparam, o que, ao menos em teoria, as forçaria a manterem sistemas de identificação de riscos (algo que já era exigido nos prospectos quando da listagem de uma empresa em bolsa).

Em 2006, uma nova diretriz da Comissão Europeia solicita que no relatório anual de governança corporativa haja descrições das principais características dos sistemas de controles internos e gerenciamento de risco da companhia, porém *apenas no que tange o processo de reporte financeiro*. A mesma diretriz diz que o comitê de auditoria deve monitorar a eficácia de *todos* os controles internos, sistemas de gerenciamento de riscos e auditoria interna – o que implica na implementação desses sistemas e controles.

C.1. Leis europeias

No que diz respeito a leis de países europeus específicos, a pesquisa de Van der Elst (*idem*, p.12-15) mostra que, na Alemanha, uma lei de 1998 estipulou que os gestores devem estabelecer um sistema de reconhecimento prévio de riscos materiais. Esse sistema deve ser controlado pelos auditores, e os gestores devem reportar sobre os riscos dos desenvolvimentos futuros da companhia.

Na Dinamarca, a lei societária, que em 2011 passou a incluir o código de melhores práticas de governança corporativa, recomenda uma identificação anual dos riscos mais importantes para a empresa, além de recomendar comunicação entre o conselho supervisor e o conselho gestor (país de *dual boards*) sobre uma série de assuntos envolvendo riscos e compliance, tendo em vista a tomada de decisões do conselho supervisor.

Na França, desde 2003, como exigência do código comercial francês, o presidente do conselho de administração (ou de supervisão, no caso de *dual boards*) deve apresentar um relatório na assembleia geral ordinária sobre os procedimentos de controle interno e gerenciamento de riscos estabelecidos pela companhia. Uma reforma de 2010 buscou endereçar a comunicação entre conselhos de empresas com sistema de conselho duplo, incluindo uma notificação anual do conselho gestor ao conselho supervisor, que contém políticas estratégicas, riscos gerais e financeiros e a gestão e controle da empresa.

A OCDE (2014, p.33) identifica que na Noruega a lei corporativa atribui ao comitê de auditoria a responsabilidade pelos sistemas de controles internos, gerenciamento de riscos e auditoria interna. Além disso, leis regendo reportes financeiros obrigam *disclosure* dos sistemas de gerenciamento de riscos e controles internos no que tange o reporte financeiro apenas.

[37] "Troubled Asset Relief Program" é o nome do programa de estabilização financeira nos EUA iniciado em meio à crise de 2008.

[38] Monda, Giorgino & Mondolin (2013, p.14-15), considera que remuneração baseada em opções tende, tudo mais constante, a incitar mais a tomada de riscos do que remuneração baseada em ações, uma vez que o valor intrínseco da opção se eleva com o aumento da volatilidade.

Ainda em seu estudo sobre a revisão dos padrões de gerenciamento de riscos vis-à-vis com os princípios da OCDE da época, a Organização (p.74-76) aponta que as leis da Suíça atribuem ao conselho a responsabilidade sobre gerenciamento de riscos no caso das empresas consideradas grandes. Requerimentos mais específicos são encontrados nas regras de listagem – há exigências de *disclosure* ("pratique ou explique") sobre as estruturas de informação e controle por parte do conselho no que tange auditoria interna, gerenciamento de riscos e sistemas de informação.

C.2. Códigos de melhores práticas de governança corporativa europeus

No que diz respeito a códigos de melhores práticas de governança europeus, Van der Elst (2013, p.16-18) afirma que os códigos do Reino Unido, Holanda, Bélgica, França e Dinamarca adicionam provisões sobre o gerenciamento de riscos e controles internos que clarificam ou vão além do que é disposto em legislação.

No Reino Unido, as regras de listagem em bolsa demandam as empresas a adotarem o UK Corporate Governance Code (de formato *comply or explain*), atribuindo, ao conselho de administração, a responsabilidade por determinar a natureza e a magnitude dos riscos significativos que pretendem incorrer para atingir os objetivos estratégicos da empresa. O código ainda especifica que o conselho deveria, ao menos anualmente, realizar uma revisão da eficácia dos sistemas de gerenciamento de risco e controles internos em seus aspectos materiais, além de reportar aos acionistas.

Mais especificamente, o código holandês assinala ao conselho supervisor o dever de monitorar a estratégia corporativa e os riscos inerentes às atividades do negócio, a eficácia dos sistemas de gestão de risco e controles internos, o processo de reporte financeiro e o *compliance* com a legislação primária e secundária. O conselho gestor (devido ao "*dual boarding*") também possui responsabilidades de *compliance* e de gerir os riscos associados com as atividades da companhia e com seu financiamento. Por fim, a diretoria executiva também tem responsabilidade pela estratégia e perfil de risco associado.

Para as responsabilidades do conselho gestor, o código chega até a prescrever alguns instrumentos do sistema de gerenciamento de riscos e controles internos, tais como análises de risco dos objetivos operacionais e financeiros, um código de conduta a ser publicado no site da companhia, guias e processos para a confecção de relatórios financeiros e um sistema de reporte e monitoramento.

O código belga indica o conselho de administração responsável pela decisão sobre valores corporativos, estratégia, apetite pelo risco e políticas chave. O sistema de gerenciamento de riscos deve ser formulado pelos gestores, aprovado pelo conselho e revisado em primeira instância pelo comitê de auditoria e depois pelo conselho.

Os códigos franceses e dinamarqueses são mais enxutos. O francês cita, sem mencionar explicitamente o conselho, que a empresa deve estar equipada com procedimentos confiáveis para a avaliação de seus compromissos e riscos, com ênfase em obrigações "*off-balance*". O dinamarquês apenas requer que o conselho estabeleça procedimentos de gerenciamento de risco e controles internos.

O estudo da OCDE (2014, p.38) menciona que o código norueguês indica responsabilidades do comitê de auditoria na revisão dos processos de controle interno. Além disso, o código confere maiores responsabilidades ao conselho de administração, com descrições específicas do que constituiriam controles internos, componentes dos sistemas de controle interno a serem revisados anualmente e os temas a serem inclusos no reporte do conselho sobre os sistemas de gerenciamento de riscos e controles internos (p.34). A empresa deve ainda reportar se segue um *framework* já estabelecido para o estabelecimento de controles internos (p.36).

Ao analisar o código da Suíça (p.74; p.76-77), a OCDE avalia que naquele país o código é um guia não obrigatório ("*not binding*"), recomendando que o comitê de auditoria ou o presidente do conselho receba um relatório sobre controles internos e gerenciamento de riscos advindo da auditoria interna. O código ainda reconhece que os controles devem ser ajustáveis ao tamanho das empresas, cobrindo gerenciamento de riscos financeiros e operacionais quando assim pertinente.

D. Ásia

Em relação à Ásia, o estudo da OCDE (2014, p.51-53) indica que, em Singapura, o código de melhores práticas no modelo "pratique ou explique", revisado em 2012, é utilizado nas regras de listagem da bolsa local (apenas para listagem primária). As informações divulgadas seriam, por sua vez, exigíveis de acordo com a lei local sobre mercado de capitais (divulgação de informações falsas é considerada crime). Além disso, há um guia específico sobre gerenciamento de riscos, também de 2012, porém não obrigatório.

O código (p.54), por sua vez, atribui responsabilidade sobre os controles internos e gerenciamento de riscos (tolerância ao risco, políticas de risco e revisão da eficácia dos sistemas) ao conselho de administração. O comitê de auditoria, tradicionalmente usado pelas empresas para auxiliar o conselho no gerenciamento de riscos, também deve estar envolvido com a supervisão dos controles internos (p.55).

E. Análise comparativa entre 21 Códigos

Uma ampla análise utilizando uma amostra de 21 códigos de melhores práticas de governança corporativa (incluindo dois códigos brasileiros, o do IBGC – 4ª edição e o da Abrasca) foi realizada no âmbito do Grupo Interagentes (ver 3.1 - Normatização vigente).

Os códigos foram selecionados considerando vários critérios, de forma a abranger países da América Latina, códigos recentes, códigos de reconhecimento global e códigos de países emergentes com giro negociado em bolsa próximo ao do mercado brasileiro (volume financeiro médio dividido pela capitalização de mercado em dólares entre 2012 e 2014).

Os resultados condensados da pesquisa são apresentados na Tabela 2 abaixo. Dentre os destaques, podemos citar que na quase totalidade dos casos (excluindo os brasileiros da análise, que serão tratados mais adiante), o conselho de administração como um todo tem responsabilidade sobre gerenciamento de riscos, quando consideramos algum papel relevante na formulação/aprovação/revisão de políticas e mecanismos de gerenciamento de risco e/ou monitoramento de sua execução pelo corpo gestor.

A tônica geral é a de que os códigos não são muito prescritivos. Apenas 9,5% dos códigos indicam algum órgão executivo dedicado ao gerenciamento de riscos corporativos. As preocupações mais encontradas, além da definição de responsabilidades do conselho e dos comitês (81%), são exigências de *disclosure* (57,1%), a elaboração de uma política formal de gerenciamento de riscos (52,4%), e revisões periódicas dos sistemas de gerenciamento de riscos (42,9%).

Tabela 2 - Resumo comparativo de gerenciamento de riscos nos códigos de governança

País	Alguma responsabilidade sobre gerenciamento de riscos - conselho de administração ou a algum de seus comitês	Citações a revisões periódicas dos sistemas de gerenciamento de risco	Citações a política formal de gerenciamento de riscos	Obrigatoriedade de comitês dedicados a risco	Área específica dedicada a gerenciamento de riscos corporativos	Exigências de reporte sobre gerenciamento de riscos em relatórios/site (além do *comply or explain*)
Alemanha	Não	Não	Não	Não	Não	Não
África do Sul	Sim	Não	Sim	Não	Não	Sim
Argentina	Sim	Não	Sim	Não	Não	Sim
Austrália	Sim	Sim	Sim	Não	Não	Sim
Chile	Não	Não	Sim	Não	Não	Não
Colômbia	Sim	Não	Sim	Sim	Não	Sim
Espanha	Sim	Não	Sim	Não	Sim	Não
França	Sim	Não	Não	Não	Não	Sim
Hong Kong	Sim	Sim	Não	Não	Não	Sim
Japão	Sim	Não	Não	Não	Não	Não
Malásia	Sim	Sim	Não	Não	Não	Sim
México	Sim	Não	Não	Não	Não	Não
OCDE	Sim	Não	Sim	Não	Não	Não
Peru	Sim	Não	Sim	Não	Não	Não
Reino Unido	Sim	Sim	Não	Não	Não	Sim
Rússia	Sim	Sim	Sim	Não	Sim	Sim
Singapura	Sim	Sim	Sim	Não	Não	Sim
Suécia	Não	Não	Não	Não	Não	Não
Tailândia	Sim	Sim	Sim	Não	Não	Sim
Taiwan	Não	Sim	Não	Não	Não	Não
Turquia	Sim	Sim	Não	Sim	Não	Sim
Total (sem Brasil)	**Sim = 81,0%**	**Sim = 42,9%**	**Sim = 52,4%**	**Sim = 9,5%**	**Sim = 9,5%**	**Sim = 57,1%**

3.2. Críticas e dificuldades na normatização

A inserção dessa seção com uma lista de críticas à normatização de gerenciamento de riscos ajuda a reflexão sobre a dosagem, direção e os cuidados ao se estabelecer os requisitos. Se de um lado, como apontado pela OCDE, diretrizes muito genéricas são de pouca utilidade, por outro lado, prescrições estritas podem trazer efeitos colaterais indesejados. Utilizamos como base o *paper* de Enriques & Zetzsche (2013) por abordar críticas e temores envolvendo diferentes perspectivas.

Em seu paper, os autores criticam a chamada "juridification" [39] do gerenciamento de riscos, argumentando que tal processo reduziria o seu valor econômico:

> *Let us further clarify from the start that we do not challenge risk management as a managerial tool per se, but rather its juridification. Risk management as a managerial tool or business technology has its merits in guiding and advising corporate directors and officers decision-making. Instead, we take issue with the trend towards embedding risk management in the law. As we argue below, this process relies on legal tools that are inherently inadequate to preserve the economic value that risk management as a mere managerial tool may have*.

Comportamento dos investidores/acionistas - dentre as críticas, cita-se a sua afirmação (p.12) de que a "juridification" do gerenciamento de riscos poderia gerar uma indevida segurança *ex-ante* por parte dos participantes do mercado quanto às reais práticas das empresas (os mesmos citam a confiança demasiada nos modelos de gerenciamento de risco do setor financeiro sob a luz da crise financeira recente, indústria essa com "juridification" avançada). A "juridification" poderia ainda gerar aos tribunais um sentimento *ex-post* de que bastaria aplicar as diretrizes cabíveis e qualquer evento danoso às companhias teria deixado de acontecer, podendo acusar o conselho e o corpo gestor como negligentes de forma injustificada.

Consequências indesejadas sobre o comportamento dos conselheiros - como uma autoridade externa com poder de ingerência sobre o gerenciamento de riscos corporativos (mesmo que via regulamentações genéricas) estaria habilitada a julgar a adequação de quaisquer procedimentos gerenciais, estratégias de negócio e decisões corporativas (p.20), essa incerteza poderia gerar conservadorismo excessivo por parte dos conselheiros, prejudicando os acionistas (p.26), além de elevar a remuneração exigida por eles, devido ao aumento do seu risco legal (p.21).

Dificuldades na definição das normas - dentre as dificuldades da "juridification" do gerenciamento de riscos, os autores ressaltam as limitações do próprio processo de gerenciamento de riscos. Eles acrescentam (p.14-15) que o gerenciamento de riscos por si só gera um risco adicional – o risco de modelagem. Certos riscos são difíceis de serem quantificados e/ou mitigados, e há o problema da qualidade dos dados e da interpretação subjetiva dos modelos. [40]

Foco do gerenciamento de riscos - os autores citam o risco de a "juridification" engendrar uma tendência em direção à uniformização do gerenciamento de riscos, privilegiando a "auditabilidade" e a "*accountability*" do sistema (seria mais seguro adotar esse caminho), o que desconsideraria importantes idiossincrasias e procedimentos informais do gerenciamento de riscos (p.22). [41] Uma

[39] Em inglês, "juridification". Podemos compreender o termo como a crescente inclusão de uma matéria em códigos legais e regulamentações.

[40] Mais especificamente, os autores citam o gerenciamento de riscos operacionais (p.16-17). Há sérios problemas de quantificação, comparabilidade e vieses em bases de dados históricos ("survivorship bias" e falta de reporte de perdas de baixo valor).

[41] Bromiley *et al.* (2014, p.9) nos alertam para outros autores na literatura que enfatizam o caráter informal de muitas decisões estratégicas numa organização, o que iria de encontro à suposição do ERM de que o planejamento estratégico é formal e sistematizado. Isso poderia ser um argumento contrário à sua adoção mandatória. Mikes & Kaplan (2014, p.31) argumentam que apenas os riscos indesejáveis são passíveis de ter seu gerenciamento em algum sentido padronizado, enquanto os demais riscos (externos e atrelados à estratégia da empresa) devem evoluir de acordo com características específicas das firmas. O guidance do FRC (Council, 2014, p.3) também é contrário à definição de um approach único como uma boa prática de gerenciamento de riscos.

tendência à uniformização poderia até elevar o risco sistêmico, ao aumentar as correlações entre as respostas das empresas a um determinado evento.

A preocupação com a auditabilidade e com a "accountability" serem centrais no gerenciamento de riscos também é expressa por Power (2009, p.852) como um dos problemas associados ao ERM (quando baseados em modelos do COSO e similares). O gerenciamento de riscos deveria privilegiar a imaginação de futuros alternativos e o questionamento das hipóteses de negócio ao invés de estimular a criação de processos e rotinas organizacionais que geram confiança e conforto, porém custosos e ineficazes, de acordo com o autor.

Tendência em considerar gerenciamento de riscos distinto/apartado do gerenciamento corporativo - ao normatizar o gerenciamento de riscos (p.18), os autores apontam que o risco de as empresas passarem a considerar o gerenciamento de riscos como algo distinto/apartado do gerenciamento geral da companhia aumenta. De certa forma, essa tendência está relacionada à anterior e, mais especificamente, há o risco de levar os conselhos a fazerem um trabalho de compliance legal ao invés de pensarem fora da caixa (p.23).[42]

Aumento de custos fixos - outro problema apontado (p.30) é a elevação dos custos fixos, principalmente na implementação de ferramentas que porventura sejam necessárias unicamente para atender os requerimentos, o que impactaria em especial as firmas menores.

3.3. Práticas internacionais

Bromiley *et al*. (2014) nos chamam a atenção para uma dificuldade na avaliação das práticas de gerenciamento de risco corporativo. Mais precisamente, nos avisa que a forma pela qual os gestores avaliam e consideram os riscos pode diferir das medidas objetivas de risco (risco de cauda, por exemplo) (p.6). Isto porque os gestores podem avaliar subjetivamente os riscos e os cenários, não se prendendo a métricas objetivas, mais comuns no setor financeiro.

Essa seção mostra algumas diretrizes mais específicas que materializam o gerenciamento de riscos, porém sem serem estritos, bem como apresenta o estágio de adoção de gerenciamento de riscos pelas empresas.

Diretrizes específicas

Muito embora seja contrário a um approach único, o *guidance* do FRC britânico (FRC, 2014) lista algumas práticas que poderiam auxiliar o cumprimento das responsabilidades nele delimitadas.

Por exemplo, em auxílio à avaliação de riscos, o *guidance* (p.6) recomenda ao conselho de administração determinar previamente a quantidade e o escopo das reuniões sobre estratégia e riscos, além de recomendar a avaliação do impacto de mudanças de estratégia, projetos e compromissos chave sobre o perfil de risco da empresa.

Aconselha ainda verificar (p.9): (i) a natureza, abrangência e apetite pelos riscos; (ii) a probabilidade e os impactos de cada risco; (iii) a capacidade da empresa em intervir e as consequências das intervenções; (iv) uma análise de custo-benefício dos controles internos; e (v) a relação entre valores,

[42] A OCDE (2014, p.44-45), ao analisar o gerenciamento de risco corporativo na Noruega, aponta que o *disclosure* sobre fatores de risco pode se tornar demasiadamente curto e genérico devido ao medo de se comprometer legalmente.

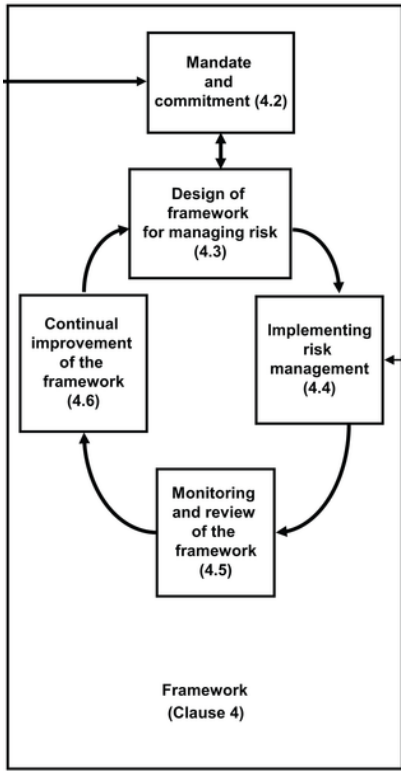
cultura e organização interna no que tange à eficácia dos controles internos e sistemas de gerenciamento de risco.

Ao aconselhar a comunicação de riscos (p.6), o guia diz que o conselho deveria especificar a natureza, fonte, formato e frequência das informações que deseja, além de verificar as suposições dos modelos que lastreiam tais informações e monitorar sua qualidade. No reporte de fatores de risco, aconselha (p.13) a inclusão de riscos, probabilidades, impactos, gerenciamento e mudanças significativas nas categorizações.

Finalmente, ao aconselhar a revisão anual da eficácia dos sistemas de gerenciamento de riscos e controles internos, o *guidance* (p.10) apoia o conselho a considerar: (i) o apetite de risco da empresa e o enraizamento da cultura de risco desejada; (ii) a determinação dos riscos principais, possíveis alterações nas suas características e a capacidade da empresa para responder às mesmas; (iii) a operação dos controles estabelecidos; (iv) a integração da gestão de risco dentro do planejamento estratégico; (v) questões especificamente identificadas nos relatórios periódicos; e (vi) a eficácia dos processos de apresentação de relatórios públicos e a comunicação entre a administração e o conselho.

O ISO 31000, por seu papel de estabelecer padrões internacionais, tem uma abordagem de apontar princípios e práticas gerais, com o intuito de tornar o gerenciamento de riscos efetivo. Conforme mencionado no capítulo 2, a estrutura conceitual de gerenciamento de riscos, no ISO 31000 (ISO, 2009), significa o *conjunto de componentes que fornecem as fundações (política, objetivos, mandato e comprometimento para administrar o risco) e os arranjos organizacionais (planos, relações, responsabilidades, recursos, processos e atividades) por desenhar, implementar, monitorar, revisar e melhorar continuamente as atividades coordenadas para direcionar e controlar uma organização no que refere a riscos*. Abaixo pode ser visto o diagrama de relacionamento entre os diversos componentes do *framework* (estrutura conceitual).

Figura 1 – Estrutura conceitual (framework) do ISO 31000 (gerenciamento de riscos)



No que interessa especificamente a essa seção do relatório, cujo objetivo é apontar algumas diretrizes que possam materializar melhor "gerenciamento de riscos", destacaríamos em:

- Mandato e comprometimento: a necessidade de atribuir a responsabilidade sobre o *framework* à alta administração, conselho e/ou gestores, para que haja comprometimento de toda organização. Assim, a alta administração é responsável por desenhar, implementar, monitorar, revisar e melhorar continuamente o gerenciamento de riscos, ressaltando-se a responsabilidade pela definição e o endosso da política de gerenciamento de riscos e pelo alinhamento dos objetivos do gerenciamento de riscos com os objetivos e estratégias da organização.
- Desenho do *framework*: a necessidade do entendimento prévio sobre os contextos interno e externo; o estabelecimento de mecanismos de comunicação e reporte; e a formulação da política de gerenciamento de riscos. A política de gerenciamento de risco é definida no ISO 31000 como a declaração da organização sobre as intenções e direcionamento gerais em relação ao gerenciamento de riscos e deve conter claramente os objetivos do gerenciamento de riscos, assim como o comprometimento da organização. Mais concretamente, a política, geralmente, aborda o racional da organização para administrar riscos; a ligação entre os objetivos da organização e a política de gerenciamento; as responsabilidades dos diversos órgãos e níveis da empresa; a forma em que o desempenho de todo o sistema de gerenciamento de riscos é mensurado, além de seu reporte, e o comprometimento de disponibilizar recursos às atividades, de revisar e melhorar a política e o *framework* de gerenciamento de riscos.
- Implementação de gerenciamento de riscos: a referência à implementação do processo de gerenciamento de riscos. O processo é entendido como a aplicação sistemática de políticas, procedimentos e práticas nas atividades de comunicação, consulta e estabelecimento de contexto, assim como nas atividades de identificação, análise, avaliação, tratamento, monitoramento e revisão de riscos. No estabelecimento do contexto, a organização considera os seus objetivos e define os parâmetros (internos e externos) na administração de riscos, além de definir os critérios de risco para avaliar a significância de um risco.
- Monitoramento e revisão do *framework*: inclui a mensuração do desempenho e do progresso de gerenciamento de riscos, respectivamente, em relação a indicadores e aos planos de gerenciamento de risco; reporte sobre riscos, progressos na execução do plano e da política de gerenciamento de riscos, e revisão do *framework*, política e planos de gerenciamento de riscos, considerando os contextos interno e externo.
- Melhoria contínua do *framework*: refere-se às decisões sobre como o *framework*, a política e os planos de ação podem ser melhorados, o que fortalece a construção da cultura de gerenciamento de riscos dentro da organização.

Vale notar, por fim, que a IFAC (2015, p.8-9) chama a atenção para alguns erros comuns no gerenciamento de riscos. Dentre eles, é enfatizada a confusão de gerenciamento de riscos com atividades de compliance, a consideração apenas do risco de perdas (o bom gerenciamento deve ponderar também os riscos de ganhos nas estratégias), controles internos focados apenas no reporte financeiro, o tratamento do gerenciamento de riscos como uma função apartada das demais e, finalmente, a imposição *top-down* de uma cultura de gerenciamento de riscos contraposta a uma mudança de mentalidade *bottom-up*.

Estágio atual de adoção de gerenciamento de riscos

Mesmo com a existência de diversos *frameworks*, diretrizes e pesquisas empíricas já analisadas, há evidências de que a adoção de gerenciamento de riscos na prática das empresas ainda não está plenamente disseminada.

Estudo de 2010 da KPMG com 203 empresas (OCDE, 2014, p.56) mostra que a maioria das empresas de Singapura pretendia adotar o ERM, porém 1/3 não havia definido um apetite pelo risco, e a maioria delas não possuía um *dashboard* de riscos organizacional. Dentre os fatores que inibirem o desenvolvimento do gerenciamento de riscos, encontram-se a indisponibilidade de dados de forma tempestiva e restrições de mão de obra e de investimentos. Já uma pesquisa do mesmo ano realizada pela bolsa de Singapura (p.59) mostra que praticamente a totalidade das empresas possuía uma política de riscos, porém apenas 27% adotavam uma terminologia e um conjunto padrões uniformes dentro da organização.

Com base em informações de uma pesquisa global da consultoria McKinsey realizada em 2011 (em OCDE, 2014, p.13), envolvendo entrevistados de cerca de 1500 companhias, a OCDE reporta que 44% dos entrevistados responderam que os conselhos de administração apenas revisavam propostas de gerenciamento de risco elaboradas pelos gestores. Além disso, apenas 14% do tempo do conselho era dedicado ao gerenciamento de riscos, o mesmo percentual dos entrevistados que alegaram possuir conhecimento pleno dos riscos enfrentados pela companhia. A OCDE (*idem*, p.18) ainda afirma que, em 2010, no conjunto dos países membros da OCDE (excluindo as companhias da Nova Zelândia, da Austrália e da Suíça; incluindo o Brasil, apesar de não ser país membro), 20% das empresas pesquisadas possuíam um comitê com referência ao gerenciamento de riscos.

Esse estudo (*idem*, p.74-75) também analisa alguns aspectos apresentados por empresas suíças. Muito embora não seja exigência regulatória, diversas empresas utilizavam *frameworks* de *standards*, em especial o ISO 31000. Uma pesquisa de 2012 da consultoria Deloitte ali citada (p.80) mostra que a maioria das empresas do índice SMI (Swiss Market Index, 47 empresas analisadas) possuía um Chief Risk Officer ou equivalente. Por fim, com base na mesma pesquisa (p.81), nota-se também que há uma tendência do disclosure sobre riscos serem genéricos e amplos, apenas o suficiente para atender às exigências regulatórias, sendo eles mais detalhados nos prospectos de distribuição de valores mobiliários.

Van der Elst (2013, p.25), aponta as conclusões de um estudo da Dutch Monitoring Commission Corporate Governance de que um número significativo (40%) de empresas holandesas apenas cumpriam tecnicamente os requerimentos normativos relacionados ao dever do conselho pelo monitoramento dos fatores de riscos (ao invés de irem além do exigido). Tal cumprimento meramente técnico seria ainda maior para os sistemas de gerenciamento de riscos e de controles internos (61%).

No que diz respeito à Noruega, o mesmo estudo da OCDE (2014, p. 39-40) nota práticas tais como o uso de mapas de risco e um sistema mais descentralizado de gerenciamento de riscos, no qual o gerente de cada unidade de negócios é o "dono" do risco. Nota também (p.43) que a intervenção do Estado nas empresas em que participa estaria focada na nomeação dos conselheiros, sem interferência nos negócios (inclusive no gerenciamento de riscos), estes conduzidos com o objetivo de maximização dos lucros, sujeito a algumas restrições previamente definidas.

Uma recente pesquisa global conduzida pela seguradora AON (2015) fornece mais informações. A pesquisa foi realizada no último trimestre de 2014, com 1418 empresas clientes (publicamente negociadas ou não) (p.1).

Dentre os cinco principais fatores externos às organizações que são "drivers" do gerenciamento de riscos (p.62), temos o crescente escrutínio dos reguladores (38% das empresas mencionaram tal fator), a volatilidade econômica (37%), pressões por parte dos consumidores (26%), ameaças cibernéticas (22%) e pressões competitivas (21%).

Sobre o grau de responsabilidade dos conselhos de administração sobre o gerenciamento de riscos, apenas em 24% das empresas o conselho ou um de seus comitês não havia estabelecido (ou não sabia informar) política de gerenciamento de riscos, ainda que informais (p.63). Esse percentual tende a cair conforme o faturamento da empresa se eleva.

Apenas 25% das empresas afirmaram possuir um CRO (*Chief Risk Officer*) focado em gerenciamento de riscos, ou demonstraram interesse em criar tal posição. No entanto, 71% das empresas possuíam uma área formal de gerenciamento de riscos, número que oscila entre 58% para empresas com faturamento abaixo de US$ 1 bilhão e 96% para empresas com faturamento acima de US$ 25 bilhões.

Em primeiro lugar, no tocante às formas de *identificação* de riscos por parte das companhias (*ibidem*), 74% das empresas afirmaram utilizar dois ou mais métodos para determinar riscos (p.54). A forma mais citada foram discussões do conselho ou do corpo gestor durante o planejamento anual ou reuniões específicas para avaliações de risco (63%), seguida da confiança no julgamento e experiência dos gestores seniores (62%). Ainda são citados informações de processos relacionados (compliance, auditoria interna, disclosures) (54%), sistemas organizacionais estruturados de gerenciamento de risco (46%), análises da indústria e relatórios externos (36%) e outros métodos (3%).

No que diz respeito à configuração geográfica desse grupo de respostas, no caso da América Latina, as percentagens foram menores para todos os itens, exceto o item "outros métodos" (4%), denotando um menor uso das práticas.

Considerando agora o tamanho das empresas, outra constatação é a de que o uso de sistemas organizacionais estruturados de gerenciamento de risco é menos comum em empresas com faturamento inferior a US$ 1 bi (35% de respostas, versus 60% no intervalo seguinte de US$ 1 bi a US$ 4,9 bi) (p.55).

Segundo, sobre as formas de *avaliação* de riscos (p. 54-55), 69% das empresas afirmaram utilizar métodos múltiplos para avaliar os riscos identificados. A forma mais citada foi a confiança no julgamento e experiência dos gestores seniores (65%), seguida das discussões do conselho ou corpo gestor durante o planejamento anual ou reuniões específicas para avaliações de risco (56%). Ainda são mencionados os sistemas organizacionais estruturados de gerenciamento de risco (40%), modelagem quantitativa (34%), consultorias externas (32%) e outros métodos (2%).

Novamente na distribuição geográfica, para as respostas da América Latina as percentagens foram mais baixas para todos os tópicos. Em relação ao tamanho das empresas, também na avaliação de riscos o uso de sistemas organizacionais estruturados de gerenciamento de risco foi menos comum em empresas com faturamento inferior a US$ 1 bi (30% de respostas versus 52% no intervalo seguinte de US$ 1 bi a US$ 4,9 bi).

Outro tópico abordado na pesquisa foram os *critérios utilizados pelas empresas para definir se um risco será ou não transferido* (p.56). O critério mais citado (59%) correspondeu à confiança nos julgamentos e experiência dos gestores seniores, seguido pelas recomendações de corretores (da seguradora) e consultores independentes (57%). Outros critérios incluíram análises de custo-benefício (49%), critérios de *benchmarks* (47%), dados de sinistro da indústria (32%), análises de cenário (28%) e outros (3%).

Por último, a pesquisa perguntou sobre os métodos usados para *avaliar a eficácia do sistema de gerenciamento de riscos* (p.64). A comparação de resultados históricos com os planos existentes nas firmas foi a alternativa mais citada (36%). Em seguida, o mapeamento interno do escopo do

gerenciamento de riscos obteve 34% de respostas, enquanto a redução no TCOR[43] obteve 32%. Além dessas alternativas, foram citadas a comparação de resultados históricos de programas de segurança e controle de perdas (31%), a avaliação do custo de oportunidade de investimentos possíveis em função de melhor gerenciamento de riscos (12%), a identificação de renda e/ou outros benefícios gerados por seguradoras cativas (9%) e outros mecanismos (5%). No entanto, 29% dos pesquisados responderem que não mensuravam a eficácia do gerenciamento de riscos.

Ainda sobre a avaliação da eficácia dos sistemas de gerenciamento de riscos, conclui-se (p.65) que a avaliação da eficácia é menos comum nas empresas com faturamento inferior a US$ 1 bilhão. Além disso, a contabilização de reduções no TCOR é expressivamente maior no caso de empresas com faturamento superior a US$ 1 bilhão.

Vale também citar o estudo de Mikes & Kaplan (2014) por possuir conteúdo distinto e mais específico que os demais. Foram selecionadas três empresas com boas práticas na governança corporativa no gerenciamento de riscos, adotadas em função de uma reestruturação dos processos internos de gerenciamento de riscos. [44]

O estudo (p.14) aborda três casos os quais após a reestruturação mencionada desembocaram em programas de ERM considerados evoluídos pelos autores, cujas características incluíam ter mais de cinco, ir visivelmente além de *checklists* e procedimentos de compliance, demonstrar envolvimento entre diversos níveis e setores organizacionais, ter o apoio da alta administração e a presença de um líder representado por um executivo sênior com linha direta ao CEO e outros executivos "C".

Com a reestruturação de processos, verificou-se que o gerenciamento de riscos havia migrado de supervisor independente do silo para parceiro de negócio, de facilitador independente (abrangendo toda a organização) ou um misto de ambos (p.24).

Na companhia de tecnologia aeroespacial escolhida, o líder do processo de gerenciamento de riscos conduzia reuniões iniciais e periódicas sobre riscos ao longo dos projetos e atrelava orçamentos a análises de risco (p.16). Na empresa do setor elétrico escolhida, o líder do processo organizou workshops de risco abrangendo diversos setores, orquestrou a construção de mapas de risco, conduziu entrevistas com executivos para reporte ao conselho, além de ter conduzido o processo de alocação de investimento em projetos que envolviam redução de risco, conforme discutidos em workshop (p.19).

Finalmente, na gestora de investimentos analisada, o gerenciamento de riscos parou de ser feito por profissionais de *compliance* para ser desempenhado por consultores independentes de riscos, cuja missão era a de elevar o retorno ajustado ao risco das carteiras, reportando tanto ao gestor de portfólio quanto ao seu superior de riscos (p.21-22).

[43] "Total Cost Of Risk" (TCOR) é uma medida que soma os custos de transferência de riscos (com seguros, derivativos), riscos de retenção (perdas realizadas), custos operacionais internos e externos à firma e ligados ao gerenciamento de riscos.

[44] Em sua opinião (p.9-10), diversos estudos empíricos sofrem de deficiências na mensuração da adoção do ERM. Esta, ao consistir num processo em evolução dentro de organizações complexas e diferentes, não deveria resultar em variáveis *dummy* homogêneas e simplistas. Sua revisão de literatura enfatiza que diversos programas de ERM possuem características distintas, alguns focando mais no uso de instrumentos financeiros, outros mais em uma avaliação holística de riscos e outros mais em *compliance* (p.10-11).

4. Panorama nacional

4.1. Normatização

A lei societária brasileira (Lei 6.404/76) não fornece nenhum comando específico relativo a gerenciamento de riscos e controles internos, embora haja dispositivos de caráter geral referentes a deveres dos administradores[45,46] e dos órgãos técnicos e consultivos, estes últimos com ênfase no conselho fiscal.

Por sua vez, a CVM emitiu algumas normas que referem a riscos, gerenciamento de riscos e controles internos para companhias registradas, além de recomendações constantes dos códigos de melhores práticas de governança corporativa do IBGC e da Abrasca.

Esse capítulo tem importância especial, uma vez que o objetivo deste nosso trabalho é identificar eventuais melhorias que possam ser feitas, seja em normas da CVM, seja no futuro Código Brasileiro, que está sendo elaborado com base no código do IBGC e na forma do código da Abrasca, ou seja, no formato Pratique ou Explique.

4.1.1. Normas da CVM

Os requerimentos legais que abordam o *disclosure* sobre **gerenciamento de riscos e controles internos para companhias com registro na CVM** podem ser encontrados na ICVM 480/09 (e alterações vincendas em janeiro/2016 conferidas pela ICVM 552/14).[47] A ICVM 308/99, entre outras matérias trata dos deveres aos auditores independentes e a ICVM 509/11 refere-se à figura do Comitê de Auditoria Estatutário.

a) ICVM 480/09 e ICVM 552/14

A ICVM 480/09, dentro outros assuntos, dispõe em seu Anexo XXIV sobre o Formulário de Referência (doravante FRE), um documento periódico enviado pelas companhias contendo uma série de informações de interesse dos investidores, entre elas informações sobre controladores e administradores, além de informações jurídicas, cadastrais e financeiras.[48]

Em 2014, foi emitida a ICVM 552, que entrará em vigor em janeiro de 2016. Dentre outros dispositivos, ampliou algumas informações prestadas no FRE no que se refere a riscos, gerenciamento de riscos e controles internos. Além disso, essas informações foram organizadas na mesma seção ou em seções sequenciais (seções 4 e 5 do FRE).

[45] O Artigo 142 da referida Lei versa sobre o dever dos conselhos de administração de "fixar a orientação geral dos negócios", eleger e fiscalizar o trabalho dos diretores e de se manifestar sobre o relatório da administração e as contas da diretoria.
[46] Deveres de diligência conferidos nos Artigos 153 e 154.
[47] De forma tangencial, a Instrução 400/03, que versa sobre distribuições públicas de valores mobiliários, solicita em seu Anexo III (item 4.1) das companhias emissoras a divulgação, em ordem de relevância, dos fatores de risco relacionados com a oferta e com o valor mobiliário que "possam, de alguma forma, fundamentar decisão de investimento de potencial investidor, devendo ser considerado no horizonte de análise de risco o prazo do investimento e do valor mobiliário distribuído e a cultura financeira dos investidores destinatários da oferta".
[48] Algumas informações solicitadas são facultativas aos emissores enquadrados na categoria "B" – apenas valores mobiliários que não configurem participação acionária.

Todos os comentários a seguir consideram as alterações como dadas, ou seja, as seções 4 e 5 da **ICVM 480 com as alterações da ICVM 552.** Para aqueles que desejarem conhecer quais foram as alterações/acréscimos, eles podem ser encontrados no Anexo 1 – Itens do Formulário de Referência – alterações em negrito

, onde comparam-se as exigências informacionais da ICVM 480 com as alterações e as da ICVM 480 sem as alterações.

A seção 4 trata de informações sobre fatores de risco, por exemplo, riscos societários, riscos regulatórios, riscos com a operação, riscos de mercado e riscos legais.

- No item 4.1, solicita-se às empresas que descrevam os fatores de risco que possam influenciar a decisão de investimento por parte dos investidores (exceto riscos de mercado e legais), sendo fornecida uma lista não exaustiva de alguns fatores de risco potencialmente relevantes, entre eles riscos societários, regulatórios, com a operação e riscos socioambientais. Por sua vez, a descrição sobre os fatores de riscos relacionados ao mercado, tais como juros e câmbio, é prestada no item 4.2. Destaca-se que o OFÍCIO-CIRCULAR/CVM/SEP/Nº02/2015 (p.125) orienta as empresas que, na descrição, os fatores de risco sejam apresentados em ordem de relevância. Assim, nos itens 4.1 e 4.2 tem-se a apresentação dos principais riscos.
- Os itens 4.3 a 4.7 referem-se a informações de diversas modalidades de processos judiciais, administrativos ou arbitrais, indicando valores envolvidos, práticas do emissor ou de sua controlada que causaram tal contingência, chances de perda, análise de impacto em caso de perda e valores provisionados. Em suma, tratam de informações sobre risco legal. Ainda, a Instrução solicita que o emissor aponte os processos que sejam relevantes para os seus negócios e os de suas controladas, devendo a relevância ser aferida levando-se em consideração a capacidade que a informação teria de influenciar a decisão dos investidores.
- O item 4.8, por sua vez, versa sobre emissores estrangeiros. Essas informações buscam fornecer ao público o conhecimento sobre as condições e as possíveis restrições ao usufruto dos direitos dos detentores de valores, devido a regras de países estrangeiros (países de emissão ou custódia).

A seção 5 trata de informações sobre gerenciamento de riscos e controles internos. Os itens 5.1 e 5.2 abordam gerenciamento de riscos e controles internos (no âmbito de gerenciamento de riscos), respectivamente, pensando-se nos riscos descritos nos itens 4.1(principais riscos, exceto riscos de mercado) e 4.2 (principais riscos de mercado); enquanto que o item 5.3 aborda controles internos no contexto de elaboração de demonstrações financeiras confiáveis e o item 5.4, alterações nos principais riscos e na política de gerenciamento de riscos.

- As informações dos itens 5.1.a e 5.2.a dizem respeito ao *disclosure* da existência ou não de uma política formalizada de gerenciamento de riscos. Caso negativo, a companhia deve explicar a razão por não possuir uma política formalizada. Caso afirmativo, a empresa deve informar qual o órgão responsável pela sua aprovação, bem como a data da sua aprovação.
- Em havendo uma política formalizada, as empresas são solicitadas a informarem, nos itens 5.1.b e 5.2.b, os objetivos e as estratégias da política de gerenciamento de riscos, inclusive informando os riscos para os quais se buscam proteção, os instrumentos utilizados para proteção e a estrutura organizacional.[49]

[49] "No caso de 5.2.b "Em relação aos riscos de mercado indicados no item 4.2, informar os objetivos e estratégias da política de gerenciamento de riscos de mercado, quando houver, incluindo (...)", por tratar-se de riscos de mercado, as empresas devem também incluir nas informações a estratégia de hedge e os parâmetros utilizados para o gerenciamento de risco.

- Nos itens 5.1c e 5.2.c, as companhias devem informar a adequação da estrutura operacional e controles internos na verificação da efetividade da política.
- O item 5.3 do FRE solicita informações mais detalhadas sobre controles internos **relativos à elaboração de informações financeiras confiáveis**, devendo a empresa informar suas principais práticas e o grau de eficiência de tais controles; as estruturas organizacionais envolvidas; se a administração (conselho e/ou diretoria) supervisiona controles internos e como ocorre a supervisão; e as deficiências e recomendações sobre controles internos presentes no relatório circunstanciado do auditor independente (ver adiante), bem como comentários dos diretores sobre as deficiências apontadas nesse relatório e as ações corretivas adotadas.
- No item 5.4 deve ser informado, em relação ao último exercício social, se houve alterações significativas nos principais riscos ou na política de gerenciamento de riscos. Também devem ser comentadas eventuais expectativas de redução ou aumento desses riscos.

Além das seções 4 e 5, abordadas anteriormente, há outras seções no FRE que podem fornecer informações indiretas sobre riscos e o seu gerenciamento. Por exemplo, a seção 7 (atividades do emissor) contém informações sobre o contexto econômico e operacional do emissor, principalmente no que diz respeito ao risco regulatório. [50]

Da mesma forma, a seção 10, onde os diretores devem fornecer aos investidores comentários (sua visão geral) dos negócios do emissor e dos fatores subjacentes ao resultado de suas operações e de sua situação financeira durante o período coberto pelas demonstrações financeiras, pode fornecer informações complementares sobre os riscos aos quais a companhia está exposta. O item 10.2, por exemplo, requer que os diretores comentem sobre "fatores que afetaram materialmente os resultados operacionais", sobre "variações das receitas atribuíveis a modificações de preços, taxas de câmbio, inflação, alterações de volumes e introdução de novos produtos e serviços" e sobre "impacto da inflação, da variação de preços dos principais insumos e produtos, do câmbio e da taxa de juros no resultado operacional e no resultado financeiro do emissor, quando relevante".

No item 10.5, os diretores devem comentar políticas contábeis críticas adotadas, em especial, estimativas contábeis feitas pela administração sobre questões incertas e relevantes para a descrição da situação financeira e dos resultados que exijam julgamentos subjetivos ou complexos. Por sua vez, o item 10.6 trata de itens relevantes não evidenciados nas demonstrações financeiras do emissor (*off-balance sheet items*).

A seção 12, sobre estrutura administrativa, trata das atribuições do conselho de administração, seus comitês e da diretoria, devendo mencionar as atribuições ligadas a gerenciamento de riscos e controles internos, caso haja. Especificamente, os comitês ou estruturas assemelhadas que participam da política de gerenciamento de riscos do emissor são descritos nos itens 12.1"a" e 12.7 do FRE.

Outra informação relevante para melhor compreender o gerenciamento de risco está na seção 13 - remuneração dos administradores. A política de remuneração pode incentivar maior ou menor disposição à tomada de risco por parte de importantes órgãos organizacionais.[51]

[50] Item "7.5" – "descrever os efeitos relevantes da regulação estatal (...)".

[51] Como bem ressalta a nota de rodapé 23 do FRE da ICVM 480/09 (correspondendo à nota 25 após as alterações da ICVM 552/14):

> "As informações sobre a política de remuneração devem abranger comitês de auditoria, de risco, financeiro e de remuneração, bem como estruturas organizacionais assemelhadas, ainda que tais comitês ou estruturas não sejam

b) ICVM 308/99 e ICVM 509/11

A ICVM 308/99 dispõe sobre o registro e o exercício da atividade de auditoria independente no âmbito do mercado de valores mobiliários. De acordo com o Artigo 20 da Instrução, os auditores independentes devem observar as normas do CFC[52], bem como os pronunciamentos técnicos do IBRACON[53]. Além disso, a Instrução explicita que os mesmos deverão "elaborar e encaminhar à administração e, quando solicitado, ao Conselho Fiscal, relatório circunstanciado que contenha suas observações a respeito de deficiências ou ineficácia dos controles internos e dos procedimentos contábeis da entidade auditada". [54]

No que diz respeito às normas de auditoria emitidas pelo CFC, a NBC TA 200 [55] (item 7) diz que cabe ao auditor identificar o risco de que as demonstrações contábeis contenham distorção relevante antes da auditoria. De forma complementar, a NBC TA 315 [56] (itens 2 e 3) explicita que a responsabilidade do auditor independente, ao desempenhar auditoria contábil, está no nível das demonstrações financeiras. Adicionalmente, a norma diz que os controles internos podem abranger demonstrações contábeis, compliance e operações (item 4), porém cabe ao auditor julgar quais são os controles relevantes para o escopo de sua auditoria (item 12).

De acordo com esta norma (item 15), a avaliação de riscos realizada pelo auditor está ligada à certificação dos processos de identificação dos riscos de negócio relevantes que afetam as demonstrações contábeis por parte da empresa. Se o auditor identificar riscos de distorção relevante que a administração deixou de identificar, ele deve julgar se cabia aos processos vigentes de controle essa identificação. Caso positivo, o auditor deve entender as causas e avaliar se os processos vigentes de controle são apropriados ou então deve determinar se há uma deficiência significativa nos controles internos (itens 16 e 17).

Finalmente, a NBC TA 265 [57] prevê que o auditor pode identificar deficiências durante qualquer etapa da auditoria, devendo comunicar por escrito as deficiências significativas aos responsáveis pela governança e podendo comunicar verbalmente as demais (itens 2; 8 e 9).

Pelo exposto acima, podemos concluir que, no que refere a controles internos, a atuação do auditor independente é focada nos riscos e controles relativos à produção de informações contábeis confiáveis.

Anteriormente à ICVM 509/11, o auditor independente não podia prestar serviços de auditoria para um mesmo cliente por prazo superior a cinco anos consecutivos, exigindo-se um intervalo mínimo de três anos para a sua recontratação.

Com as alterações promovidas por essa instrução, permitiu–se que esse seja estendido para 10 anos, desde que a companhia auditada possua Comitê de Auditoria Estatutário (CAE) [58] em funcionamento permanente e que o auditor independente seja pessoa jurídica.[59]

---

estatutários, desde que tais comitês ou estruturas participem do processo de decisão dos órgãos de administração ou de gestão do emissor como consultores ou fiscais."

[52] Conselho Federal de Contabilidade.
[53] Instituto dos Auditores Independentes do Brasil.
[54] Artigo 25, inciso II.
[55] NBC TA 200 - Objetivos gerais do auditor independente e a condução da auditoria em conformidade com normas de auditoria.
[56] NBC TA 315 - Identificação e avaliação dos riscos de distorção relevante por meio do entendimento da entidade e do seu ambiente.
[57] NBC TA 265 - Comunicação de deficiências de controle interno.

Por sua vez, o CAE, dentre outras atribuições [60], deve supervisionar as atividades da área de controles internos, da área de auditoria interna e da área de elaboração das demonstrações financeiras da companhia. Deve ainda monitorar a qualidade e integridade dos mecanismos de controles internos e das informações trimestrais, demonstrações intermediárias e demonstrações financeiras da companhia.[61]

Por fim, o CAE deve avaliar e monitorar as exposições de risco da companhia, podendo inclusive requerer informações detalhadas de políticas e procedimentos relacionados com a remuneração da administração, utilização de ativos da companhia e as despesas incorridas em nome da companhia.[62] Contudo, tal tarefa de avaliação e monitoramento das exposições de risco possui um enfoque mais de emissão de opinião sobre a eficácia dos processos de controles internos e interface com os trabalhos das auditorias independentes.

Ou seja, com a ICVM 509/11 incentiva-se a existência de um órgão estatutário vinculado ao conselho de administração com responsabilidades sobre controles internos e a qualidade e integridade da elaboração de demonstrações financeiras. No entanto, trata-se de um órgão com uma ênfase em controles, ao passo que o gerenciamento de riscos prescinde da estratégia corporativa e possui dinâmica diferente.

Em resumo, as normas da CVM demandam amplo *disclosure* dos principais riscos financeiros e não financeiros. Em relação a gerenciamento de riscos, há a solicitação de informação sobre a existência de uma política formalizada ou não (inclusive a explicação das razões, caso não houver); o órgão responsável pela sua aprovação, bem como os objetivos e as estratégias dessa política, incluindo os riscos para os quais se busca a proteção, os instrumentos utilizados na proteção e como o gerenciamento de riscos se estrutura na organização. Adicionalmente é solicitada a informação de como a estrutura operacional e de controles internos está adequada para verificar a efetividade da política de gerenciamento. No que refere a controles internos no âmbito de elaboração de demonstrações contábeis confiáveis, além de amplo *disclosure*, há normas específicas sobre o assunto.

4.1.2. Códigos e manuais de melhores práticas de governança corporativa

Enquanto que as normas da CVM referentes a gerenciamento de riscos tratam de *disclosure*, os dois códigos atualmente existentes no Brasil têm caráter de fornecer diretrizes ou recomendações, principalmente em relação à responsabilidade dos órgãos de administração. No entanto, o código de IBGC constitui-se mais num guia de boas práticas de governança, enquanto que o código da Abrasca tem o formato de "pratique ou explique".

a) Código das melhores práticas de governança corporativa (IBGC)

Fundado em 27/11/1995, o IBGC "é uma organização exclusivamente dedicada à promoção da Governança Corporativa no Brasil e o principal fomentador das práticas e discussões sobre o tema no

[58] Órgão de conselho previsto em estatuto, composto por no mínimo três membros indicados pelo conselho de administração, sendo vedada a participação de diretores da companhia, suas controladas, controladora, coligadas ou sociedades em controle comum, diretas ou indiretas, e composto em sua maioria por membros independentes.
[59] Art.31-A, Incisos I e II.
[60] Art.31-D, Inciso II, Alíneas "b)", "c)" e "d)".
[61] Art.31-D, Inciso III, Alíneas "a)" e "b)".
[62] Art.31-F, Inciso IV, Alíneas "a)", "b)" e "c)".

País, tendo alcançado reconhecimento nacional e internacional" (IBGC, 2009, p.4). Como a 4ª edição do código está em processo de revisão, neste trabalho utilizamos a **versão proposta do código, que foi colocada em audiência pública em julho de 2015. No que refere a gerenciamento de riscos, exceto por realocações, não há alterações relevantes entre a versão proposta e a 4ª edição.**

De acordo com a versão proposta (IBGC, 2015), as responsabilidades do conselho de administração, do seu comitê de auditoria [63] e da diretoria em relação a gerenciamento de riscos podem ser encontradas em vários trechos do código, dividindo-se em fundamentos e práticas:

- "O conselho deve assegurar-se de que a diretoria identifica preventivamente – por meio de um sistema de informações adequado – e lista os principais riscos aos quais a organização está exposta, além de sua probabilidade de ocorrência, a exposição financeira consolidada desses riscos (considerando a probabilidade de ocorrência, o impacto financeiro potencial e os aspectos intangíveis) e as medidas e os procedimentos adotados para sua prevenção ou mitigação" – prática (p. 105).
- "É o conselho de administração quem aprova políticas específicas para o estabelecimento dos limites aceitáveis para exposição da organização a esses riscos. Também acompanha e assegura que a diretoria possua mecanismos e controles internos para conhecer, avaliar e controlar os riscos, de forma a mantê-los em níveis compatíveis com os limites fixados" – fundamento (p. 84).
- "Assegurar que a gestão identifique, mitigue e monitore os riscos da organização" – fundamento (p. 29).
- "O comitê de auditoria tem como objetivo dar o suporte ao conselho de administração nas seguintes atividades sob a sua responsabilidade: c) supervisionar a estrutura e as atividades de gerenciamento de riscos pela gestão da companhia, abrangendo os riscos operacionais, financeiros, estratégicos e de imagem, em linha com as diretrizes e políticas estabelecidas pelo conselho de administração (...)" – fundamento (p55).
- "A diretoria deve executar as diretrizes gerais fixadas pelo conselho de administração e ser responsável pela elaboração e implementação de todos os processos operacionais e financeiros, inclusive os relacionados à gestão de risco..." – prática (p. 77).

No que tange a controles internos e compliance:

- "O comitê de auditoria tem como objetivo dar o suporte ao conselho de administração nas seguintes atividades sob a sua responsabilidade [do conselho]: a) monitoramento da efetividade e a qualidade dos controles internos da organização...; b) monitoramento do cumprimento a regras, leis e regulamentos (compliance) pela gestão..." - fundamento (p. 55).
- "A diretoria, auxiliada pelos órgãos de controle vinculados ao conselho de administração (como o comitê de auditoria e a auditoria interna), deve construir e operar sistemas de controles internos eficazes para o monitoramento dos processos operacionais e financeiros, inclusive os relacionados com a gestão de riscos e de conformidade (compliance), assim como para o controle da comunicação com o mercado e demais *stakeholders*" – prática (p. 84).
- "No mínimo anualmente, a diretoria deve rever tais sistemas [os mencionados no *bullet* anterior] quanto à sua eficácia, e prestar contas ao conselho de administração sobre essa avaliação" – prática (p. 85).
- "A diretoria deve garantir que os sistemas de controles internos estimulem a adoção, por parte dos órgãos internos encarregados de monitorar e fiscalizar as atividades da organização, de

[63] Preferencialmente formado somente por conselheiros e não deve ter executivos em sua composição - prática (p. 53).

atitudes preventivas, prospectivas e proativas na minimização e antecipação de riscos" – prática (p.85).

- "O comitê de auditoria deve tratar com os auditores independentes [sobre] os principais riscos e deficiências relevantes e falhas significativas nos controles internos" – prática (p. 58).
- "O comitê de auditoria e o conselho de administração devem avaliar as respostas e ações da diretoria sobre as recomendações de controles internos apresentadas pelos auditores [independentes]" – prática (p. 95)

b) Código Abrasca de autorregulação e boas práticas das companhias abertas (Abrasca)

De acordo com seu *website*[64], a "principal missão da Associação Brasileira das Companhias Abertas – Abrasca – associação civil sem fins lucrativos criada em 21 de dezembro de 1971 – é a defesa, em sua atuação conjunta, das posições da companhia aberta, como a face moderna da economia brasileira, junto aos centros de decisão e à opinião pública".

Seu código de melhores práticas é de adesão voluntária, contratual e de caráter "pratique ou explique" (Abrasca, 2015, p.4). Ao adotarem contratualmente o código, as empresas automaticamente aderem ao Código Processual de Autorregulação Abrasca, recebendo um selo de distinção (p.34). Atualmente 23 empresas adotam o código, sendo que sete destas ou são holdings ou são ligadas ao setor financeiro. [65]

Para entendimento do código, é importante notar que ele apresenta princípios, recomendações e regras. Os dois primeiros não exigem prática ou explicação, isto é o "pratique ou explique" refere-se às regras.

Diversas recomendações (ou regras) em relação a responsabilidades do conselho de administração, do comitê de auditoria[66] e da diretoria, tratam o gerenciamento de riscos em conjunto com controles internos, conforme pode ser visto a seguir:

- O código estabelece como "regra" que o conselho de administração deve aprovar uma política de controles internos e gestão de riscos - regra (5.1) e princípio (p. 17). Adicionalmente, o conselho é responsável por estabelecer as políticas e os limites para os riscos operacionais e financeiros – regra (3.1.2) (p.12).
- O código da Abrasca confere ao conselho de administração as responsabilidades de "monitorar as atividades da diretoria e o gerenciamento de riscos" e "zelar pela confiabilidade das informações financeiras e estratégicas e para que os controles financeiros e os sistemas de administração de risco sejam adequados e efetivamente aplicados" - princípio (p.6).
- Os comitês são vistos como órgãos de assessoria do conselho e devem ser presididos por um conselheiro, podendo ser integrados por pessoas internas ou externas [67] - regra (2.4.3, p.10-11).

---

[64] <http://www.abrasca.org.br/Abrasca/Missao-Objetivos> Acesso em 12/08/2015.

[65] <http://www.abrasca.org.br/Autorregulacao/Companhias-que-Aderiram-ao-Codigo> Acesso em 21/09/2015.

[66] Segundo a ABRASCA:

> "é recomendável que o comitê de auditoria, se instalado, tenha entre seus membros ao menos um especialista em finanças e um Conselheiro Independente, podendo o especialista em finanças ser o Conselheiro Independente; e seja composto majoritariamente por Conselheiros Independentes, Conselheiros Não Executivos ou membros externos que preencham os requisitos de independência aplicáveis aos Conselheiros Independentes" (ABRASCA, 2015, p. 19).

[67] É importante notar que apesar da existência de "regras" em relação a comitês quanto à gestão de risco e aos controles internos, o código não pressupõe a existência deles, afirmando como princípio básico que o "conselho

- Recomenda-se "a participação de ao menos um conselheiro independente nos comitês que tenham por atribuição questões de controles internos e gestão de riscos" - recomendação (2.4.8, p.11), e se um comitê do conselho identificar "deficiência ou desconformidade relevante nos sistemas de controles internos e gestão de risco da Companhia, o conselho de administração deve imediatamente avaliar a situação e, caso a recomendação do comitê seja aprovada, exigir da diretoria a correção da referida deficiência ou desconformidade" - regra (2.4.7, idem).
- O comitê de auditoria deve ainda avaliar a efetividade e suficiência dos sistemas de controle e gerenciamento de riscos, e, finalmente, se manifestar "previamente ao conselho de administração, a respeito do relatório anual sobre o sistema de controles internos e de gerenciamento de riscos corporativos da Companhia" – recomendação (5.7.1, p.18).
- A diretoria é responsável pelos sistemas de controles internos e gestão de riscos - regra (5.2) (p.17).

Mais especificamente sobre controles internos e *compliance*, têm-se:

- Os sistemas de controles internos e de gestão de riscos "devem estimular todas as pessoas encarregadas de monitorar e fiscalizar os processos operacionais e financeiros a adotarem uma atitude preventiva, prospectiva e pró-ativa no controle de riscos" - regra (5.3, p.17).
- O código afirma que os controles internos devem "permitir à administração monitorar os processos operacionais e financeiros, assim como os riscos de desconformidade com as políticas e os limites estabelecidos pelo conselho de administração" - princípio (*idem*).
- Adicionalmente, a empresa "deve ter uma área voltada para acompanhar a eficácia dos controles internos e a observância de regras prudenciais por todos os administradores, empregados e outros colaboradores" - regra (5.5, p.18).
- O comitê de auditoria, caso existente, deve avaliar a efetividade e a suficiência da estrutura de controles internos e dos processos de auditoria interna e independente da Companhia, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias – recomendação (5.7.1, *idem*).
- Ainda sobre os controles, o conselho de administração ou o órgão competente "deve, ao menos anualmente, reunir-se com os auditores independentes e revisar e discutir o relatório de deficiências e recomendações sobre os controles internos emitidos pelos auditores independentes e as correspondentes respostas da diretoria, bem como deliberar acerca de qualquer proposta de modificação ou aprimoramento dos sistemas de controles internos submetida pelo diretor-presidente" - regra (5.4, p.17).

c) Resumo

A tabela a seguir resume as disposições de ambos os códigos.

---

de administração deve considerar a criação de comitês de assessoramento, para assuntos complexos e especializados" - princípio (p.10).

Tabela 3 - Estrutura conceitual das diretrizes de gerenciamento de riscos, controles internos e compliance - códigos brasileiros.

	IBGC (IBGC, 2015)	Abrasca
Responsabilidades - políticas/limites	O conselho de administração estabelece as diretrizes e políticas sobre a estrutura e as atividades de gerenciamento de riscos (fundamento, p. 55) e aprova políticas específicas para o estabelecimento dos limites aceitáveis de exposição aos principais riscos (fundamento, p. 84).	O conselho de administração aprova política de controles internos e gerenciamento de riscos financeiros e não financeiros (regra 5.1 e princípio p. 17). Também é responsável por estabelecer as políticas e os limites para os riscos operacionais e financeiros (regra 3.1.2).
Responsabilidades – implementação	O conselho de administração deve assegurar que a diretoria identifique e liste os principais riscos, além de sua probabilidade de ocorrência, a exposição financeira desses riscos (considerando a probabilidade de ocorrência, o impacto financeiro potencial e os aspectos intangíveis), bem como as medidas e os procedimentos adotados para sua prevenção ou mitigação (prática, p. 105). Também, deve acompanhar e assegurar que a diretoria possua mecanismos e controles internos para conhecer, avaliar e controlar os riscos para mantê-los em níveis compatíveis com os limites fixados (fundamento, p. 84).	
Responsabilidades - monitoramento	Além de assegurar que a gestão identifique e mitigue riscos, o conselho também deve assegurar que a gestão monitore os riscos da organização (fundamento, p. 84), devendo esta construir e operar sistemas de controles internos para o monitoramento dos processos operacionais e financeiros, inclusive os relacionados com a gestão de riscos e de compliance (prática, p. 84). O comitê de auditoria, se instalado, deve auxiliar o conselho ao supervisionar estrutura e atividades de gerenciamento de riscos financeiros *e não financeiros* por parte da diretoria executiva. Deve ainda auxiliar o conselho ao monitorar a efetividade e a qualidade dos controles internos da organização e a execução do compliance pela diretoria executiva (fundamento, p. 55).	O conselho de administração deve monitorar as atividades de gerenciamento de riscos da diretoria executiva e zelar pela confiabilidade das informações financeiras e estratégicas e pela adequação e efetiva aplicação dos sistemas de controles internos e gerenciamento de riscos (princípio, p. 6). O comitê de auditoria, se instalado, deve avaliar a efetividade e suficiência dos sistemas de controle e gerenciamento de riscos. Deve ainda se manifestar previamente ao conselho de administração, a respeito do relatório anual sobre o sistema de controles internos e de gerenciamento de riscos (recomendação 5.71). O conselho de administração deve imediatamente avaliar e exigir correções por parte da diretoria executiva se um de seus comitês identificar deficiência ou desconformidade relevante nos sistemas

		de controles internos e gerenciamento de riscos, no caso da recomendação do comitê ser aprovada (regra 2.4.7).
Responsabilidades – execução	Cabe à diretoria executiva executar diretrizes gerais do conselho e ser responsável pela elaboração e implementação de todos os processos operacionais e financeiros, inclusive os relacionados à gestão de riscos (prática, p. 77). Deve construir e operar sistemas de controles internos para o monitoramento dos processos operacionais e financeiros, inclusive os relacionados com a gestão de riscos e de compliance (prática, p. 84). Ver outros detalhes sobre responsabilidades da diretoria nos itens "implementação" e "monitoramento", citados acima.	A diretoria é responsável pelos sistemas de controles internos e gestão de riscos (regra 5.2). A empresa deve ter uma área voltada para acompanhar a eficácia dos controles internos (regra 5.5). Entende-se que controles internos permitem à administração monitorar os processos operacionais e financeiros, assim como os riscos de desconformidade com as políticas e os limites estabelecidos pelo conselho de administração (princípio, p.17).
Revisão de sistemas	Anualmente a diretoria deve rever os sistemas de gerenciamento de riscos, controles internos e compliance, quanto à sua eficácia, e prestar contas ao conselho de administração sobre essa avaliação (prática, p.85).	
Relacionamento do conselho de administração com auditores	O comitê de auditoria, caso existente, deve tratar com os auditores independentes sobre os principais riscos, deficiências relevantes e falhas significativas nos controles internos [no contexto da preparação das dem. Financeiras] (prática, p.85). O comitê de auditoria, caso existente, ***e*** *o conselho de administração* devem avaliar as respostas e ações da diretoria sobre as recomendações de controles internos apresentadas pelos auditores independentes (prática, p. 95).	O comitê de auditoria, caso existente, deve avaliar a efetividade e a suficiência dos processos de auditoria interna e independente da Companhia, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos (recomendação 5.7.1). O conselho de administração **ou** o órgão competente deve, ao menos anualmente, reunir-se com os auditores independentes e revisar e discutir o relatório de deficiências e recomendações sobre os controles internos emitidos pelos últimos e as correspondentes respostas da diretoria (regra 5.4).

Com base na tabela, pode-se notar que o principal foco dos dois códigos diz respeito à atribuição de responsabilidades, em geral sem orientações mais específicas sobre os componentes de gerenciamento de riscos, ou então, pode-se notar a existência de poucas orientações consideradas "práticas" (IBGC) ou "regras" (Abrasca) e, portanto, sujeitas ao "praticar ou explicar", que a construção do Código Brasileiro de Governança Corporativa pretende endereçar. Particularmente, esses aspectos serão tratados no capítulo "Conclusão".

Porém há diferenças na intensidade de foco e de envolvimento do conselho de administração no desenvolvimento do gerenciamento de riscos, mesmo quando os dois códigos aparentam ser similares. Por exemplo, o código do IBGC parece atribuir um envolvimento maior ao conselho, ao indicar que este órgão deve estabelecer as diretrizes e políticas de gerenciamento de riscos, enquanto que no da Abrasca a tarefa do conselho é o de aprovação da política. Também, o código do IBGC aponta que o

conselho deve aprovar políticas específicas de limites para os principais riscos, ao mesmo tempo em que o da Abrasca cita apenas os riscos operacionais e financeiros.

Destaca-se que ambos os códigos indicam a diretoria como responsável pela execução de gerenciamento de riscos e controles internos, por meio de construção de sistemas para tais finalidades. Vale também mencionar que o conceito de controles internos em ambos os códigos vai além daqueles que incluem apenas controles internos direcionados para a preparação confiável de informações financeiras.

Por fim, o código do IBGC detalha mais a estrutura de gerenciamento de riscos (explicitando a identificação de riscos e sua avaliação; medidas e procedimentos de prevenção e de mitigação; e revisão dos sistemas de gerenciamento), enquanto que o código da Abrasca foca quase que exclusivamente em monitoramento.

4.2. Práticas de empresas brasileiras

Para obtermos uma fotografia, ainda que bastante parcial, das práticas de gerenciamento de risco nas empresas brasileiras, foi realizado um levantamento das informações prestadas no FRE pelas 17 maiores empresas cujas ações fazem parte do índice Ibovespa, em termos de capitalização de mercado (excluindo as financeiras[68]). As informações foram coletadas ao longo de agosto de 2015, portanto ainda sem as alterações introduzidas pela ICVM 522/14. O conjunto de informações consideradas relevantes para o escopo deste trabalho encontra-se no Anexo 2.

Assim, é provável que o reporte de muitas dessas empresas sobre gerenciamento de riscos tenha se **restringido a informações exclusivamente relacionadas riscos de mercado**, uma vez que não eram solicitadas informações relativas a gerenciamento de outros riscos. Dentre as informações analisadas, destacamos as responsabilidades do conselho e dos comitês em nível de conselho, as responsabilidades em nível da diretoria executiva, características gerais das políticas e práticas de gerenciamento de riscos de mercado e controles internos, além de práticas de gerenciamento de riscos que não sejam riscos de mercado (este último de forma bem limitada, conforme mencionado acima).

Em suas respostas, algumas empresas deram a entender que o gerenciamento de riscos vai além dos riscos de mercado, ainda que a exigência normativa atual não solicite tal informação.[69] De acordo com a Tabela 5, das 17 empresas, duas delas não relataram a existência de uma política de gerenciamento de riscos de mercado, conforme exigido pelo item 5.2 do FRE. Das demais quinze empresas, uma delas (Eletrobras) não relatou o órgão responsável, ao passo que uma delas reportou que a diretoria financeira é a responsável (Telefonica Brasil). As treze demais reportaram que a responsabilidade cabe ao conselho de administração. Ressalta-se novamente que o uso do termo gerenciamento de riscos significa a sua formulação/ definição/estrutura (ou seja, não se trata neste caso de execução).

Das treze empresas que conferem responsabilidades sobre gerenciamento de riscos ao conselho de administração, uma delas (Kroton) atribuiu essa responsabilidade ao comitê de auditoria. Cinco empresas atribuíram ao conselho como um todo (sem citação a comitês adicionais), enquanto as demais sete empresas citaram, além do conselho de administração, um ou mais de seus comitês (padrão mais comum nas empresas de maior capitalização de mercado).

[68] Itausa também foi excluída, uma vez que o gerenciamento de riscos é tratado junto com a controlada.
[69] Foram elas: Ambev, Petrobras, BRF, Vale, Embraer, Fibria.

Adicionalmente, as respostas tendem a mencionar como papel do conselho de administração apenas a definição de políticas e limites. Apenas sete (de treze) respostas (Ambev, Petrobras, BRF, JBS, Embraer, CCR, Kroton) mencionaram explicitamente que o conselho e seus comitês possuem papel de monitoramento do processo de gerenciamento de riscos (ainda que de mercado).

No que diz respeito ao trabalho da diretoria, é interessante notar que cinco empresas reportaram o uso de comitês de risco para administrar os riscos de mercado (Tabela 5).

Em parte, devido aos requisitos normativos que só exigirão informações mais detalhadas sobre riscos não financeiros com a entrada em vigor da Instrução 552/14, as referências às características gerais das políticas e práticas de gerenciamento de riscos focaram nos riscos de mercado. Ainda assim, algumas empresas citaram de forma voluntária algumas práticas gerais. De acordo com a Tabela 7, pode-se notar que uma companhia (Fibria) voluntariamente menciona a adoção da metodologia de ERM, muito embora outras companhias mencionem "análise interconectada de riscos financeiros para definição de estratégias" (Ambev), análise "multidisciplinar" (Lojas Renner), fluxos parecidos com o do ERM (Suzano), ou então que o gerenciamento de riscos inclui "riscos empresariais, operacionais, mercadológicos, de governança e legal" (Embraer).

No que diz respeito a controles internos e compliance (Tabela 8), seis empresas mencionaram a utilização da metodologia do COSO para verificação da eficácia dos controles internos. Vale também ressaltar que os reportes focam mais na estrutura organizacional do que nas práticas efetivas.

Em relação a práticas de gerenciamento de riscos não financeiros (ou não de mercado), embora o reporte não fosse obrigatório, várias companhias forneceram voluntariamente algumas informações, porém, novamente, bastante limitadas. Os riscos abordados estão compilados na Tabela 9. Apenas duas empresas não reportaram nada que se encaixasse nesse tópico. Algumas das informações sobre demais riscos dizem respeito a investimentos e precauções tomadas para evitar riscos ambientais. Vale a pena ressaltar os reportes de Embraer, Lojas Renner e Souza Cruz, que mencionaram de maneira mais ampla ferramentas de mitigação para riscos não financeiros.

5. Conclusão

Considerando os princípios, pode-se afirmar que os códigos de governança existentes atualmente no Brasil alinham-se com os Princípios da OCDE no que tange a gerenciamento de riscos. Os princípios da OCDE especificam o conselho de administração da empresa como responsável por direcionar, monitorar e revisar as políticas e procedimentos de gerenciamento de riscos, bem como por assegurar a integridade dos reportes contábeis e financeiros e a existência de controles internos adequados. Ao mesmo tempo, os princípios deixam claro que o corpo executivo é responsável por administrar os riscos. Ainda, os princípios da OCDE apontam a necessidade de se estabelecer o grau de risco aceito pela empresa frente aos seus objetivos e como esta irá gerenciar os riscos inerentes a suas operações e relações.

Princípios são diretrizes essenciais, porém, como o próprio nome diz, são necessariamente genéricos. Portanto, pode haver a necessidade de materializá-los em práticas operacionais mais concretas para que possam ser úteis tanto para as empresas quanto para a informação direcionada aos investidores. Conforme mencionado no Capítulo 1 - Introdução, este trabalho busca verificar eventuais lacunas que, se trabalhadas, poderiam contribuir para aperfeiçoamentos no *disclosure* que a CVM já requer das empresas, mas principalmente visa a contribuir para os debates do futuro Código Brasileiro de Governança Corporativa, que está sendo elaborado pelo Grupo Interagentes. Também, como afirmado anteriormente, esse Código está sendo formatado na forma de Pratique ou Explique e pretende-se que seja mandatoriamente aplicável ao menos às empresas brasileiras com ações publicamente negociadas.

A OCDE menciona em seus princípios a divulgação dos riscos relevantes e dos sistemas utilizados para monitorar e gerenciar os riscos. Sob a perspectiva de a empresa prover informações de qualidade sobre riscos, gerenciamento de riscos e controles internos (estes como parte integral ou parcial do gerenciamento de riscos), alguma abrangência e profundidade precisa ser indicada. Afinal, no contexto de um Código Pratique ou Explique, se uma empresa afirma que adota determinada prática/recomendação/princípio, a informação só pode ter qualidade caso traga evidências de como determinada prática é adotada.

Um ponto de atenção é a clarificação entre os papéis dos controles internos, do *compliance* e do gerenciamento de riscos. Independentemente de como a empresa se organiza, ao se dar o *disclosure*, é necessário algum direcionamento sobre o que deve ser considerado em cada uma dessas funções, por exemplo, na forma como fez o FRE da ICVM 480, especificando alguns elementos sobre política de gerenciamento de riscos na seção 5.

No Capítulo 2, este trabalho mostra que é praticamente consenso que *compliance* faz parte do sistema de controles internos. Por sua vez, a nosso ver, controles internos tem intersecção com gerenciamento de risco – e é esta parte que nos interessa neste estudo.[70] Mais especificamente, nos interessam os principais riscos, ou seja, aqueles que podem afetar de alguma forma a evolução da empresa. Sendo assim, acreditamos que o futuro Código Brasileiro de Governança Corporativa (pratique ou explique) deve ser claro, explicitando os contornos de cada função, de forma a evitar que as empresas acreditem estar reportando gerenciamento de riscos quando estão referindo-se basicamente a controles internos ou *compliance*. Deve ainda explicitar claramente a cobertura de gerenciamento de riscos (riscos financeiros e riscos não financeiros) e dos controles internos (geral e não apenas uma parcela dos controles internos, por exemplo, controles internos relativos à elaboração de demonstrações financeiras confiáveis).

[70] As visões diferenciam-se: alguns autores afirmam que controles internos estão integralmente inseridos em gerenciamento de riscos, enquanto que outros preferem tratá-los como parcialmente.

Outro ponto importante para que os investidores possam fazer uma avaliação sobre os principais riscos e o gerenciamento de riscos da empresa (incorporando parte dos controles internos que nos interessa no estudo), será importante a indicação de práticas mínimas que devem ser atendidas para a empresa afirmar que adota gerenciamento de riscos. Porém, como buscamos alertar ao longo do texto, as empresas são diferentes entre si, o que significa que, diante das suas particularidades, muito possivelmente se estruturam de forma diferente para gerenciar riscos.

Abaixo, em formato de tabela, listamos algumas diretrizes/práticas apresentadas no Capítulo 3 que, em nossa opinião, podem servir ao propósito de materializar melhor os princípios, contudo sem afetar a flexibilidade das empresas adotarem os seus próprios processos e modelos. A tabela tem basicamente a sequência da estrutura do ISO 31000, que é bastante didática.

Uma vez que o conteúdo do Código do IBGC será utilizado como base do futuro Código Brasileiro de Governança Corporativa, e que possivelmente o Formulário de Referência será utilizado como veículo de reporte para as empresas, também é apresentada uma comparação entre as diretrizes/práticas listadas e os tópicos correspondentes na versão do Código do IBGC que foi colocada em audiência pública em julho e na versão da ICVM 480 alterada pela ICVM 522. Finalmente, com os comentários, concluímos sobre as lacunas que a nosso ver poderiam ser preenchidas, tendo em vista o Código Brasileiro de Governança Corporativa, no formato pratique ou explique.

Tabela 4 – Conclusão: diretrizes/práticas versus códigos e normas da CVM

Diretrizes/práticas	Código do IBGC, ICVM 480 e comentários
• Definição dos órgãos da alta administração responsáveis pela definição do desenho, implementação, monitoramento e revisão do gerenciamento de riscos, bem como a responsabilidade pela execução dos processos.	O Código do IBGC aponta o conselho como responsável de uma forma geral pela definição, implementação e monitoramento de diretrizes e políticas sobre a estrutura e as atividades de gerenciamento de riscos, cabendo (p. 77) à diretoria executiva a execução, sendo esta a responsável pela elaboração e implementação de todos os processos relacionados à gestão de risco. A ICVM 480 prevê, na seção 12 (sobre estrutura administrativa), que sejam informadas as atribuições do conselho, de seus comitês e da diretoria em relação a gerenciamento de riscos e controles internos, caso haja. O mesmo se aplica a outros comitês ou estruturas assemelhadas. <u>Comentário</u>: é necessário notar que, no Código do IBGC, alguns itens estão na forma de fundamentos, enquanto que outros na forma de práticas. O mesmo se repete em outros tópicos.
• Desenho do *framework* do gerenciamento de riscos implica na formulação de uma política de gerenciamento de riscos, contendo a ligação entre os objetivos da organização e a política de gerenciamento, as responsabilidades dos diversos órgãos e	Há menção no Código do IBGC de **diretrizes e políticas sobre a estrutura e as atividades de gerenciamento de riscos** (fundamento, p.55).[71] A ICVM 480 (itens 5.1.b, 5.2.b, 5.1.c e 5.2.c), embora com redação diferente, requer

[71] O Código da Abrasca menciona a existência da politica de gerenciamento de riscos, porém não há nenhuma especificação sobre o seu conteúdo.

níveis da estrutura da empresa, a forma em que o desempenho de todo o sistema de gerenciamento de riscos é mensurado, entre outros.	informação bem completa sobre política de gerenciamento de riscos (caso seja formalizada), incluindo os objetivos e as estratégias da política de gerenciamento de riscos; os riscos para os quais se busca proteção e os instrumentos utilizados; a estrutura organizacional; e a adequação da estrutura operacional e controles internos na verificação a efetividade da política. Comentário: as diretrizes e políticas sobre a estrutura e as atividades de gerenciamento de riscos do Código do IBGC poderiam ser concretizadas no Código Brasileiro, por exemplo, por meio de uma política de gerenciamento de riscos, contendo basicamente os elementos da ICVM 480 (ou elementos similares).
• Implementação do processo de gerenciamento de riscos, destacando-se a aplicação sistemática de políticas, procedimentos e práticas nas atividades de identificação, análise, avaliação e tratamento de riscos. Além disso, destacam-se a abordagem sobre os parâmetros na administração de riscos e os critérios de risco utilizados para avaliar a sua significância.	O Código do IBGC prevê que o conselho deve assegurar que a diretoria identifique e liste os principais riscos, além de sua probabilidade de ocorrência, a exposição financeira desses riscos (considerando a probabilidade de ocorrência, o impacto financeiro potencial e os aspectos intangíveis), bem como as medidas e os procedimentos adotados para sua prevenção ou mitigação (prática, p. 105). Adicionalmente, diz como fundamento que o conselho aprova políticas específicas para o estabelecimento dos limites aceitáveis de exposição aos principais riscos (p. 84). A ICVM 480 requer que a empresa aponte/identifique seus principais riscos (não mercado e mercado) nos itens 4.1 e 4.2. Adicionalmente, os itens 5.1.b e 5.2.b incluem os instrumentos utilizados para proteção. Comentário: além de identificação e listagem dos principais riscos e as medidas e procedimentos e parâmetros adotados para seu tratamento (que deveria ser mais amplo que prevenção ou mitigação), a redação da prática e do fundamento do Código do IBGC, juntos, poderia ser ajustada para o Código Brasileiro, por exemplo, para permitir outros métodos de identificação e análise de riscos que não o de matriz probabilidade X impacto. Alternativamente, poderiam ser inseridas referências mais genéricas sobre a existência de um processo sistemático de identificação, análise e avaliação de riscos, com critérios, com a especificação do Código do IBGC como um exemplo.
• Monitoramento, incluindo como o desempenho e o progresso de gerenciamento de riscos é avaliado; e o fluxo dos reportes (principalmente para os responsáveis finais) sobre riscos, os progressos na execução do	O Código do IBGC diz que o conselho deve assegurar que a gestão monitore os riscos da organização (fundamento, p. 84), devendo esta construir e operar sistemas de controles internos eficazes para o monitoramento dos processos

planejado e da política de gerenciamento de riscos.	operacionais e financeiros, inclusive os relacionados com a gestão de riscos e de *compliance* (prática, p. 84). Adicionalmente, o comitê de auditoria, se instalado, deve auxiliar o conselho ao supervisionar estrutura e atividades de gerenciamento de riscos financeiros *e não financeiros* por parte da diretoria executiva. Deve ainda auxiliar o conselho a monitorar a efetividade e a qualidade dos controles internos da organização e a execução do compliance pela diretoria executiva (fundamento, p. 55). A ICVM 480, conforme mencionado acima, prevê, na seção 12 (sobre estrutura administrativa), que sejam informadas as atribuições do conselho, de seus comitês e da diretoria em relação a gerenciamento de riscos e controles internos, caso haja. O mesmo se aplica a outros comitês ou estruturas assemelhadas. Além disso, os itens 5.1.c e 5.2.c endereçam a adequação da estrutura operacional e controles internos na verificação da efetividade da política. Comentário: o monitoramento e supervisão referidos no Código do IBGC poderiam ser mais bem concretizados no Código Brasileiro, fazendo menção explícita à forma de avaliação sobre o desempenho e o progresso de gerenciamento de riscos; e reportes sobre riscos e progressos na execução do planejado e da política de gerenciamento de riscos, incluindo o desempenho e as práticas dos controles internos, quanto à sua efetividade.
• Revisão anual da eficácia da política de gerenciamento de riscos e dos sistemas, incluindo a atribuição de responsabilidade pelo processo de revisão, o próprio processo e os resultados.	O Código do IBGC prevê que anualmente a diretoria deve rever os sistemas de gerenciamento de riscos, controles internos e *compliance*, quanto à sua eficácia, e prestar contas ao conselho de administração sobre essa avaliação (prática, p. 85). A ICVM 480 (item 5.4) requer que o emissor informe, em relação ao último exercício social, se houve alterações significativas nos principais riscos ou na política de gerenciamento de riscos. Também devem ser comentadas eventuais expectativas de redução ou aumento desses riscos. Comentário: para complementar o tópico sobre revisão, o Código Brasileiro poderia acrescentar a revisão sobre a política de gerenciamento de riscos e os principais riscos, explicitando as expectativas quanto a seu aumento ou redução.

• Controles internos gerais	Os comentários acima abrangem os controles internos no contexto de gerenciamento de riscos.
• Tópico específico sobre controles internos no âmbito de elaboração de demonstrações financeiras confiáveis	O Código do IBGC diz que o diretor presidente, em conjunto com a diretoria é responsável pela elaboração e proposição para aprovação do conselho de administração de sistemas de controles internos voltados a monitorar o cumprimento dos processos operacionais e financeiros, assim com os riscos de não conformidade (fundamento, p.104). Ao mesmo tempo, o Código do IBGC apresenta como prática na página 84 que a gestão deve construir e operar sistemas de controles internos eficazes para o monitoramento dos processos operacionais e financeiros, inclusive os relacionados com a gestão de riscos e de *compliance*. Portanto, pode se dizer que o tópico é coberto duplamente, como fundamento e como prática. Adicionalmente, o conselho, com o suporte do comitê de auditoria, tem sob a sua responsabilidade o monitoramento da efetividade e qualidade dos controles internos (fundamento, p. 55), sendo que a eficácia desses sistemas deve ser revista no mínimo anualmente (prática, p. 104). Além disso, de acordo com o Código, o comitê de auditoria deve tratar com os auditores independentes os principais riscos e deficiências relevantes e falhas significativas nos controles internos (prática, p. 58) e que o comitê de auditoria e o conselho de administração devem avaliar as respostas e ações da diretoria sobre as recomendações de controles internos apresentados pelos auditores independentes (prática, p. 95). A ICVM 480 (item 5.3) solicita informações detalhadas, devendo a empresa informar suas principais práticas e o grau de eficiência de tais controles, as estruturas organizacionais envolvidas, se a administração supervisiona controles internos e como ocorre a supervisão, e as deficiências e recomendações sobre controles internos presentes no relatório circunstanciado do auditor independente, além de comentários dos diretores sobre as deficiências apontadas no relatório o auditor independente e as ações corretivas adotadas. <u>Comentário</u>: tanto o Código do IBGC quanto a ICVM 480 são bastante completos nesse tópico e compatíveis entre si.

Referências bibliográficas

AON (2015). *Global Risk Management Survey 2015*. < http://www.aon.com/2015GlobalRisk/attachments/2015-Global-Risk-Management-Report-230415.pdf> Acesso em 28/08/2015.

Associação Brasileira das Companhias Abertas (Abrasca) (2015 [2011]). *Código Abrasca de autorregulação e boas práticas das companhias abertas*. < http://www.abrasca.org.br/Uploads/autoregulacao/codigo_Abrasca_de_Autorregulacao_e_Boas_Praticas_das_Companhias_Abertas.pdf>. Acesso em 12/08/2015.

Bertinetti, G. S., Cavezzali, E., & Gardenal, G. (2013). The effect of the enterprise risk management implementation on the firm value of European companies. *Department of Management, Università Ca'Foscari Venezia Working Paper*, (10).

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2014). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*. Disponível em SSRN: http://ssrn.com/abstract=2376261

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise risk management – Integrated Framework*. Committee of the Sponsoring Organizations of the Treadway Commission.

Cheffins, B. R. (2013). *The history of corporate governance*. Oxford Handbook Of Corporate Governance, Oxford University Press, 2013.

Enriques, L., & Zetzsche, D. (2013). The Risky Business of Regulating Risk Management in Listed Companies. *European Company and Financial Law Review*, *10*(3), 271-303.

Financial Reporting Council (FRC) (2014). *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*. Disponível em <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pdf> Acesso em 15/08/2015.

IFAC (2015) *From Bolt-On To Built-In: Managing Risk as an Integral Part of Managing an Organization*. Disponível em <https://www.ifac.org/publications-resources/bolt-built> Acesso em 6/8/15.

Instituto Brasileiro de Governança Corporativa (IBGC) (2015). *Código das Melhores Práticas de Governança Corporativa*. 5ªed. (rascunho não publicado) / Instituto Brasileiro de Governança Corporativa.

--- (2009) *Código das Melhores Práticas de Governança Corporativa*. 4.ed. / Instituto Brasileiro de Governança Corporativa.

Ittner, C. D., & Keusch, T. (2015). The Influence of Board of Directors' Risk Oversight on Risk Management Maturity and Firm Risk-Taking. *AAA 2015 Management Accounting Section (MAS) Meeting*.

International Organization for Standardization (ISO) (2009). ISO 31000: Risk management – principles and guidelines. *Geneva, Switzerland*.

Kirkpatrick, G. (2009). Corporate governance and the financial crisis. *OECD, Financial Market Trends*, *96*(1), 1-30.

Lehuede, H. J., Kirkpatrick, G., & Teichmann, D. (2012). Corporate Governance Lessons from the Financial Crisis. Disponível em SSRN: http://ssrn.com/abstract=2393978.

John, K., Litov, L., & Yeung, B. (2008). Corporate governance and risk-taking. *The Journal of Finance*, *63*(4), 1679-1728.

Mikes, A., & Kaplan, R. S. (2014). Towards a contingency theory of enterprise risk management. *AAA 2014 Management Accounting Section (MAS) Meeting Paper*.

Miller, G. P. (2014). The compliance function: an overview. *NYU Law and Economics Research Paper*, (14-36).

Monda, B., Giorgino, M., & Modolin, I. (2013). Rationales for Corporate Risk Management - A Critical Literature Review. Disponível em SSRN: http://ssrn.com/abstract=2203546.

NCGB (Norwegian Corporate Governance Board) (2014). "The Norwegian Code of Practice for Corporate Governance." *Norway:(8th Edition, 2014)*.

OCDE (2015) *G20/OECD Principles of Corporate Governance*, Corporate Governance, OECD Publishing.

---- (2014) *Risk Management and Corporate Governance*, Corporate Governance, OECD Publishing.

---- (2004) *OECD Principles of Corporate Governance*, OECD Publishing.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6), 849-855.

Smithson, C., & Simkins, B. J. (2005). Does risk management add value? A survey of the evidence. *Journal of Applied Corporate Finance*, *17*(3), 8-17.

Standard&Poors (2013) *What Informative Evidence Does Standard & Poor's Use In Its Updated Enterprise Risk Management Analysis?* < http://www.standardandpoors.com/spf/upload/Ratings_EMEA/2013-05-08_WhatInformativeEvidenceDoesSPUse.pdf> Acesso em 29/07/2015.

Tricker, R. I. (2015). *Corporate governance: Principles, policies, and practices*. Oxford University Press, USA.

Van der Elst, C. (2013). The Risk Management Duties of the Board of Directors. *Financial Law Institute Working Paper Series 2013-02*.

Anexos

Anexo 1 – Itens do Formulário de Referência – alterações em negrito

ICVM 480 com alterações da ICVM 552	ICVM 480 sem alterações da ICVM 522
4. Fatores de risco	4. Fatores de risco
4.1. Descrever fatores de risco que possam influenciar a decisão de investimento, em especial, aqueles relacionados: a. ao emissor b. a seu controlador, direto ou indireto, ou grupo de controle c. a seus acionistas d. a suas controladas e coligadas e. a seus fornecedores f. a seus clientes g. aos setores da economia nos quais o emissor atue h. à regulação dos setores em que o emissor atue i. aos países estrangeiros onde o emissor atue **j. a questões socioambientais**	4.1. Descrever fatores de risco que possam influenciar a decisão de investimento, em especial, aqueles relacionados: a. ao emissor b. a seu controlador, direto ou indireto, ou grupo de controle c. a seus acionistas d. a suas controladas e coligadas e. a seus fornecedores f. a seus clientes g. aos setores da economia nos quais o emissor atue h. à regulação dos setores em que o emissor atue i. aos países estrangeiros onde o emissor atue
4.2. Descrever, quantitativa e qualitativamente, os principais riscos de mercado a que o emissor está exposto, inclusive em relação a riscos cambiais e a taxas de juros.	5.1. Descrever, quantitativa e qualitativamente, os principais riscos de mercado a que o emissor está exposto, inclusive em relação a riscos cambiais e a taxas de juros.
4.3. Descrever os processos judiciais, administrativos ou arbitrais em que o emissor ou suas controladas sejam parte, discriminando entre trabalhistas, tributários, cíveis e outros: (i) que não estejam sob sigilo, e (ii) que sejam relevantes para os negócios do emissor ou de suas controladas, indicando: a. juízo b. instância c. data de instauração d. partes no processo **(nota: Em relação aos processos judiciais sujeitos à apreciação da Justiça do Trabalho, devem ser indicadas apenas as iniciais dos nomes das partes).** e. valores, bens ou direitos envolvidos f. principais fatos g. se a chance de perda é:	4.3.Descrever os processos judiciais, administrativos ou arbitrais em que o emissor ou suas controladas sejam parte, discriminando entre trabalhistas, tributários, cíveis e outros: (i) que não estejam sob sigilo, e (ii) que sejam relevantes para os negócios do emissor ou de suas controladas, indicando: a. juízo b. instância c. data de instauração d. partes no processo e. valores, bens ou direitos envolvidos f. principais fatos g. se a chance de perda é:

i. provável ii. possível iii. remota h. análise do impacto em caso de perda do processo	i. provável ii. possível iii. remota h. análise do impacto em caso de perda do processo
4.3.1. Indicar o valor total provisionado se houver, dos processos descritos no item 4.3	4.3.i. valor provisionado, se houver provisão
4.4. Descrever os processos judiciais, administrativos ou arbitrais, que não estejam sob sigilo, em que o emissor ou suas controladas sejam parte e cujas partes contrárias sejam administradores ou ex-administradores, controladores ou ex-controladores ou investidores do emissor ou de suas controladas, informando: a. juízo b. instância c. data de instauração d. partes no processo **(nota 7: Em relação aos processos judiciais sujeitos à apreciação da Justiça do Trabalho, devem ser indicadas apenas as iniciais dos nomes das partes).** e. valores, bens ou direitos envolvidos f. principais fatos g. se a chance de perda é: i. provável ii. possível iii. remota h. análise do impacto em caso de perda do processo	4.4. Descrever os processos judiciais, administrativos ou arbitrais, que não estejam sob sigilo, em que o emissor ou suas controladas sejam parte e cujas partes contrárias sejam administradores ou ex-administradores, controladores ou ex-controladores ou investidores do emissor ou de suas controladas, informando: a. juízo b. instância c. data de instauração d. partes no processo e. valores, bens ou direitos envolvidos f. principais fatos g. se a chance de perda é: i. provável ii. possível iii. remota h. análise do impacto em caso de perda do processo
4.4.1. Indicar o valor total provisionado, se houver, dos processos descritos no item 4.4	4.4.i valor provisionado, se houver provisão
4.5. Em relação aos processos sigilosos relevantes em que o emissor ou suas controladas sejam parte e que não tenham sido divulgados nos itens 4.3 e 4.4 acima, analisar o impacto em caso de perda e informar os valores envolvidos.	4.5. Em relação aos processos sigilosos relevantes em que o emissor ou suas controladas sejam parte e que não tenham sido divulgados nos itens 4.3 e 4.4 acima, analisar o impacto em caso de perda e informar os valores envolvidos.
4.6. Descrever os processos judiciais, administrativos ou arbitrais repetitivos ou conexos, baseados em fatos e causas jurídicas semelhantes, que não estejam sob sigilo e que em conjunto sejam relevantes, em que o emissor ou suas controladas sejam parte, discriminando entre trabalhistas, tributários, cíveis e outros, e indicando:	4.6. Descrever os processos judiciais, administrativos ou arbitrais repetitivos ou conexos, baseados em fatos e causas jurídicas semelhantes, que não estejam sob sigilo e que em conjunto sejam relevantes, em que o emissor ou suas controladas sejam parte, discriminando entre trabalhistas, tributários, cíveis e outros, e indicando:

a. valores envolvidos b. prática do emissor ou de sua controlada que causou tal contingência	a. valores envolvidos c. prática do emissor ou de sua controlada que causou tal contingência
4.6.1. Indicar o valor total provisionado, se houver, dos processos descritos no item 4.6.	4.6.b. valor provisionado, se houver
4.7. Descrever outras contingências relevantes não abrangidas pelos itens anteriores.	4.7. Descrever outras contingências relevantes não abrangidas pelos itens anteriores.
4.8. Em relação às regras do país de origem do emissor estrangeiro e às regras do país no qual os valores mobiliários do emissor estrangeiro estão custodiados, se diferente do país de origem, identificar: a. restrições impostas ao exercício de direitos políticos e econômicos b. restrições à circulação e transferência dos valores mobiliários c. hipóteses de cancelamento de registro**, bem como os direitos dos titulares de valores mobiliários nessa situação** **d. hipóteses em que os titulares de valores mobiliários terão direito de preferência na subscrição de ações, valores mobiliários lastreados em ações ou valores mobiliários conversíveis em ações, bem como das respectivas condições para o exercício desse direito, ou das hipóteses em que esse direito não é garantido, caso aplicável** e. outras questões do interesse dos investidores	4.8. Em relação às regras do país de origem do emissor estrangeiro e às regras do país no qual os valores mobiliários do emissor estrangeiro estão custodiados, se diferente do país de origem, identificar: a. restrições impostas ao exercício de direitos políticos e econômicos b. restrições à circulação e transferência dos valores mobiliários c. hipóteses de cancelamento de registro d. outras questões do interesse dos investidores
5. Política de gerenciamento de riscos e controles internos	**5. Riscos de mercado**
5.1. Em relação aos riscos indicados no item 4.1, informar: **a. se o emissor possui uma política formalizada de gerenciamento de riscos, destacando, em caso afirmativo, o órgão que a aprovou e a data de sua aprovação, e, em caso negativo, as razões pelas quais o emissor não adotou uma política** **b. os objetivos e estratégias da política de gerenciamento de riscos, quando houver, incluindo:** **i. os riscos para os quais se busca proteção** **ii. os instrumentos utilizados para proteção** **iii. a estrutura organizacional de gerenciamento de riscos**	

c. a adequação da estrutura operacional e de controles internos para verificação da efetividade da política adotada	
5.2. Em relação aos riscos de mercado indicados no item 4.2, informar: **a. se o emissor possui uma política formalizada de gerenciamento de riscos de mercado, destacando, em caso afirmativo, o órgão que a aprovou e a data de sua aprovação, e, em caso negativo, as razões pelas quais o emissor não adotou uma política** b. os objetivos e estratégias da política de gerenciamento de riscos de mercado, quando houver**, incluindo:** i. os riscos de mercado para os quais se busca proteção ii. a estratégia de proteção patrimonial (hedge) iii. os instrumentos utilizados para proteção patrimonial (hedge) iv. os parâmetros utilizados para o gerenciamento desses riscos v. se o emissor opera instrumentos financeiros com objetivos diversos de proteção patrimonial (hedge) e quais são esses objetivos vi. a estrutura organizacional de controle de gerenciamento de riscos de mercado c. a adequação da estrutura operacional e controles internos para verificação da efetividade da política adotada	5.2. Descrever a política de gerenciamento de riscos de mercado adotada pelo emissor, seus objetivos, estratégias e instrumentos, indicando: a. riscos para os quais se busca proteção b. estratégia de proteção patrimonial (hedge) c. instrumentos utilizados para proteção patrimonial (hedge) d. parâmetros utilizados para o gerenciamento desses riscos e. se o emissor opera instrumentos financeiros com objetivos diversos de proteção patrimonial (hedge) e quais são esses objetivos f. estrutura organizacional de controle de gerenciamento de riscos g. adequação da estrutura operacional e controles internos para verificação da efetividade da política adotada
5.3. Em relação aos controles adotados pelo emissor para assegurar a elaboração de demonstrações financeiras confiáveis, **indicar**: a. **as principais práticas de controles internos** e o grau de eficiência de tais controles, indicando eventuais imperfeições e as providências adotadas para corrigi-las **b. as estruturas organizacionais envolvidas** **c. se e como a eficiência dos controles internos é supervisionada pela administração do emissor, indicando o cargo das pessoas responsáveis pelo referido acompanhamento** d. deficiências e recomendações sobre os controles internos presentes no relatório circunstanciado, preparado e encaminhado ao emissor pelo auditor independente, nos termos da regulamentação emitida pela CVM que trata do registro e do exercício da	10.6. Com relação aos controles internos adotados para assegurar a elaboração de demonstrações financeiras confiáveis, os diretores devem comentar: a. grau de eficiência de tais controles, indicando eventuais imperfeições e providências adotadas para corrigi-las b. deficiências e recomendações sobre os controles internos presentes no relatório do auditor independente

atividade de auditoria independente **e. comentários dos diretores sobre as deficiências apontadas no relatório circunstanciado preparado pelo auditor independente e sobre as medidas corretivas adotadas**	
5.4. Informar se, em relação ao último exercício social, houve alterações significativas nos principais riscos a que o emissor está exposto ou na política de gerenciamento de riscos adotada**, comentando, ainda, eventuais expectativas de redução ou aumento na exposição do emissor a tais riscos**	5.3. Informar se, em relação ao último exercício social, houve alterações significativas nos principais riscos de mercado a que o emissor está exposto ou na política de gerenciamento de riscos adotada [esse item do FRE, anteriormente restringia-se apenas a riscos de mercado]
5.5. Fornecer outras informações que o emissor julgue relevantes.	5.4. Fornecer outras informações que o emissor julgue relevantes [esse item do FRE, anteriormente restringia-se apenas a riscos de mercado].

Anexo 2 – Práticas de gerenciamento de riscos das empresas brasileiras (reportes no FRE)

Tabela 5 - Estrutura organizacional de gerenciamento de riscos das empresas nacionais - papel do conselho de administração e comitês em nível de conselho.			
Empresa	**Empresa reportou existência de política formal de gerenciamento de riscos de mercado?**	**Responsabilização pela política de gerenciamento de riscos**	**Papel do conselho e comitês em nível de conselho**
Ambev	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos e monitoramento do gerenciamento de riscos. Comitê de Operações, Finanças e Remuneração: monitoramento do gerenciamento de riscos.
Petrobras	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos e monitoramento do gerenciamento de riscos. Comitê de Auditoria: assessorar o Conselho de Administração e os administradores da companhia na avaliação da adequação e da eficácia dos controles internos, com o apoio da Auditoria Interna e da auditoria independente, assim como das unidades envolvidas no gerenciamento de riscos e de controles internos da companhia. Além disso, deve assessorar o Conselho de Administração no estabelecimento de políticas globais relativas à avaliação e gerenciamento de riscos.
BRF	Sim	Conselho de Administração	Conselho de Administração: é o responsável pela aprovação da Política de Gestão de Riscos, além de definir os limites de tolerância aos diferentes riscos identificados como aceitáveis para a Companhia em nome de seus acionistas. Comitê de Finanças, Governança e Sustentabilidade: também será responsável pelo acompanhamento dos riscos não financeiros ou contábeis, incluindo riscos operacionais e outros. Adicionalmente, compete a tal Comitê assessorar o Conselho de Administração visando a assegurar o cumprimento dos mecanismos e controles relacionados à gestão de riscos financeiros, aplicações das políticas financeiras, os processos tributários, diretrizes estratégicas de captação alinhadas ao perfil de risco do negócio, considerando a adequada estrutura de capital da Companhia. Comitê de Auditoria: deve supervisionar a área de controles internos, de auditoria interna e de elaboração das demonstrações financeiras da

			Companhia. Deve monitorar a qualidade e integridade dos mecanismos de controles internos e avaliar e monitorar as exposições de risco da Companhia.
Vale	Sim	Conselho de Administração	Conselho de Administração: Define tolerância ao risco em conjunto com diretoria executiva, além de ser responsável pela política de gerenciamento de riscos. Comitê Financeiro: responsável por emitir parecer sobre as políticas de riscos da Vale e sistemas internos de controle financeiro da Vale. Conselho Fiscal: responsável por avaliar os controles internos e o sistema de gerenciamento de riscos, de maneira a apurar denúncias, assegurar a sua eficácia e adequação e dos recursos despendidos, qualificação e experiência dos responsáveis e seus programas de treinamento. Cabe ainda ao Conselho Fiscal discutir com o Auditor Externo, Auditoria Interna, Comitê de Controladoria e a Diretoria Executiva de Finanças, o resultado da avaliação do sistema de controles internos como um todo, visando ao seu aprimoramento.
JBS	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos. Comitê Financeiro e de Gestão de Riscos: nomeado pelo conselho, auxilia a Diretoria Financeira a examinar e revisar informações relacionadas com o gerenciamento de risco, incluindo políticas significativas, procedimentos e práticas aplicadas no gerenciamento de risco. Poderão integrar este comitê os membros titulares ou suplentes do Conselho de Administração da Companhia, seus Diretores; ou profissionais da área de finanças.

			Comitê de Auditoria: a pedido do Conselho de Administração deve avaliar a qualidade e eficiência dos sistemas de controles internos e de administração de riscos.
Ultrapar	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos.
Embraer	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos. Comitê de Auditoria e Riscos: tem por objetivo assessorar o Conselho de Administração, em atividades como acompanhar e avaliar os riscos empresariais, de natureza operacional, mercadológica, de imagem, de governança corporativa, financeira ou legal dos mercados administrados pela Companhia, por meio do diagnóstico das fontes de risco das atividades da Companhia, avaliar a adequação dos modelos de aferição dos riscos e validação dos modelos utilizados, analisar e opinar sobre as diretrizes e políticas da gestão de risco, sobre as informações gerenciais e contábeis divulgadas ao público e órgãos reguladores e avaliar a adequação dos recursos humanos e financeiros destinados à gestão de riscos da organização.
Telefônica Brasil	Sim	Diretoria Financeira	
Lojas Renner	Não		* Diz que a "Diretoria" avalia se o gerenciamento do negócio está em linha com as políticas e diretrizes definidas pela "Administração", não sendo clara.
CCR	Não	Muito embora o Conselho de Administração reporte seu papel relativo à políticas gerais, a política de gerenciamento de riscos de mercado não é mencionada nos reportes.	Comitê Financeiro acompanha e informa ao Conselho de Administração sobre questões financeiras chave, tais como empréstimos/refinanciamentos de dívidas de longo prazo, análise de risco de mercado, exposições ao câmbio, propostas de hedge, aval em operações, nível de alavancagem, política de dividendos, emissão de ações, emissão de títulos de dívida e investimentos. Conselho de Administração: é responsável pela definição de políticas estratégicas gerais e, entre outras atribuições, pelo estabelecimento de políticas e diretrizes gerais, por eleger nossos diretores e fiscalizar a sua gestão.

Kroton	Sim	Conselho de Administração	Comitê de Auditoria: tem a atribuição de, entre outras, coordenar a gestão de risco das atividades. Tem como missão assegurar a operacionalização dos processos à gestão de auditoria interna e da contratação da auditoria independente, dos mecanismos e controles relacionados à gestão de riscos e a coerência das políticas financeiras com as diretrizes estratégicas e o perfil de risco do negócio. No tocante ao controle de gerenciamento de riscos, compete ainda ao nosso Comitê de Auditoria tratar com os auditores independentes métodos e avaliação de risco e os resultados dessas avaliações, direcionar a nossa Diretoria na determinação de parâmetros do modelo de gestão de nossos riscos e avaliar periodicamente as políticas de gerenciamento de riscos, seus recursos e tolerância máxima a riscos, além de aprovar um plano de auditoria interna, levando em consideração a adequada cobertura de riscos.
Eletrobras	Sim	Não Reportado	
Fibria	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos. Aprova, anualmente, a revisão das políticas financeiras que estabelecem os princípios e normas para a gestão de risco global, áreas envolvidas nestas atividades, uso de instrumentos financeiros derivativos e não derivativos e alocação dos excedentes de caixa.
Souza Cruz	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos. Comitê de Auditoria e Responsabilidade Social: está autorizado pelo Conselho de Administração a avaliar os riscos do emissor (probabilidade e potencial impacto, seguindo a metodologia de supervisão baseada em risco).
Klabin	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos.
Suzano	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos.
Hypermarcas	Sim	Conselho de Administração	Conselho de Administração: aprova a política de riscos.

Tabela 6 - Estrutura organizacional de gerenciamento de riscos das empresas nacionais - papel da diretoria e seus comitês para administração de riscos.

Empresa	Empresa reportou existência de comitê dedicado ao gerenciamento de riscos de mercado?	Papel da diretoria executiva e comitês em nível de diretoria

Ambev	Não Reportado	Diretoria Financeira: executa o gerenciamento de riscos, e reporta semestralmente ao Conselho Fiscal e ao Conselho de Administração Gerência de Riscos Corporativos, responsável pelo monitoramento dos controles internos necessários para mitigar os riscos financeiros, operacionais e estratégicos inerentes às operações da Companhia, bem como assegurar a aderência às leis/regulamentações e políticas internas. A Gerência de Riscos Corporativos tem como responsabilidade reportar o resultado desta avaliação ao Diretor Presidente e ao Comitê de Auditoria, além de acompanhar os planos de ação elaborados para remediar quaisquer deficiências identificadas nos processos.
Petrobras	Não Reportado	Diretoria Financeira e de RI: possui responsabilidades sobre gerenciamento de riscos financeiros. Área de Governança, Risco e Conformidade (GRC): nova área de GRC deve fortalecer visão integrada dos riscos empresariais, em articulação com as diversas áreas e reportando a diretoria executiva e ao Conselho de Administração, além de cuidar da estruturação da governança e do compliance.
BRF	Sim	Comitê de Gestão de Riscos Financeiros: condução e aplicação diária da política de riscos. É o órgão da diretoria executiva com poder de vetar propostas em desacordo com a política de risco.
Vale	Sim	Diretoria Executiva: desenvolve instrumentos de gerenciamento de risco com base na política aprovada, além de reportar-se ao Conselho de Administração Mais especificamente, a Diretoria de Tesouraria e Finanças e engloba as áreas de Seguros e de Gestão de Risco de Mercado e Crédito, e é a área que responde pelo gerenciamento de riscos. É responsabilidade da área de gestão de riscos definir e propor ao Comitê Executivo de Gestão de Risco operações ou medidas de mitigação de riscos de mercado. Comitê Executivo de Gestão de Riscos: comitê de diretoria criado pelo Conselho de Administração para auxílio à diretoria executiva nas análises e pareceres, também atuando na supervisão e revisão dos sistemas de gerenciamento de risco.
JBS	Não Reportado	Diretor de Finanças: executa políticas de hedge. Diretoria de Controle de Riscos: mapeia riscos e leva avaliação a Comissão de Gestão de Riscos, que responde ao Conselho de Administração.

Ultrapar	Sim	Diretoria Financeira da Ultrapar: execução da política de gerenciamento de riscos financeiros, além do contínuo aprimoramento da política. Comitê de Riscos e Aplicações Financeiras: cabe a ele a supervisão e o monitoramento do cumprimento dos princípios, diretrizes e parâmetros da política de risco. Os membros do Comitê são nomeados pelo Diretor Presidente. O Comitê se reúne regularmente e tem como atribuições, entre outras, a discussão e o acompanhamento das estratégias financeiras, das exposições existentes e das operações relevantes que envolvam aplicação, captação de recursos ou mitigação de riscos. O Comitê monitora periodicamente os parâmetros de risco estabelecidos pela Política através de um mapa de acompanhamento.
Embraer	Sim	Comitê de Gestão Financeira: recebe mensalmente a posição consolidada de riscos e acompanha e analisa se a gestão dos recursos e seus respectivos riscos estão em conformidade com a Política de Gestão Financeira da Embraer. Atribuições do comitê de gestão financeira incluem analisar relatório de riscos financeiros, limites de crédito, cenários de mercado, garantias, dentre outros. Riscos e Controles Internos: trabalha de forma colaborativa com a área de Auditoria Interna e Compliance da Embraer para alinhar os riscos, planos de ação e evitar sobreposições de atividades. Realiza o reporte de suas atividades, resultados e planos de ação para o Conselho de Administração, Conselho Fiscal e Comitê de Auditoria e Riscos. Auditoria Interna: é responsável por avaliar a suficiência e a eficácia dos controles operacionais e de gestão, verificar a adequação dos processos de identificação e gerenciamento dos riscos e avaliar a eficácia dos controles relacionados à gestão contábil e a geração de relatórios financeiros.
Telefônica Brasil	Não Reportado	Gerência de Controle e Gestão de Riscos Financeiros: elabora política de gerenciamento de riscos e monitora diariamente a aderência das operações financeiras aos níveis de exposição definidos pelo comando da empresa. Diretoria de Finanças e de Relações com Investidores: aprova política de gerenciamento de riscos. Diretoria de Auditoria Interna: avalia controles internos e faz recomendações que podem fortalecer o gerenciamento de riscos.
Lojas Renner	Sim	Comitê Executivo: formado pela Diretoria e pelos gerentes gerais. Com base em uma análise de cenário que inclui riscos e oportunidades, elabora o planejamento estratégico para aprovação pelo Conselho de Administração. A partir da definição de prioridades, as estratégias são desdobradas em projetos e metas para todos os diretores e grupo de executivos.

CCR	Não Reportado	Diretoria Financeira e Tesouraria Corporativa: são responsáveis pelas operações envolvendo instrumentos financeiros.
Kroton	Não Reportado	Diretoria: propor ao Conselho de Administração políticas de riscos, alçadas e investimentos aplicáveis à Companhia.
Eletrobras	Sim	Comitê de Hedge Financeiro: é coordenado pelo diretor financeiro e é multi-áreas. Cabe a ele definir as estratégias e os instrumentos de hedge a serem apresentados à Diretoria Executiva da Eletrobras para aprovação. Comitê de Riscos: gerenciamento de riscos a nível corporativo.
Fibria	Não Reportado	Gerência Geral de Governança, Riscos e Compliance: controle dos riscos e compliance das políticas, possuindo independência para apontar eventuais desenquadramentos das políticas, mensurar e analisar os riscos de mercado, reportando diretamente ao presidente da Companhia e ao Comitê de Finanças (órgão de apoio ao Conselho de Administração). Ainda precifica derivativos, participa de comitês, elabora relatórios mensais de risco, elabora testes de estresse e simula VaRs.
Souza Cruz	Conselho de Administração	Área de Gestão de Riscos e Controles – tem como objetivo principal avaliar duas vezes ao ano os riscos da operação, a probabilidade de ocorrência, a magnitude de impacto e os controles existentes para mitigar tais riscos.
Klabin	Não Reportado	
Suzano	Não Reportado	Consultor ou Analista de Riscos - responsável pela identificação, mensuração e reporte dos valores em risco, assim como pela elaboração, em conjunto com o Gerente de Tesouraria, de estudos que subsidiem a tomada de decisões na contratação de operações para o enquadramento das exposições aos limites de risco estabelecidos, de acordo com as diretrizes do Comitê de Gestão. Gerência de Gestão de Riscos e Controles Internos: melhorar ainda mais sua estrutura de controles internos e governança corporativa. Gerente de Tesouraria: responsável pela indicação e execução de operações financeiras para a mitigação dos riscos de mercado analisados, por meio da contratação dos instrumentos financeiros disponíveis no mercado.
Hypermarcas	Não Reportado	Gestão de Riscos: responsável pela identificação e tratamento de possíveis fraudes ou atitudes inadequadas e por riscos inerentes aos processos, esses juntamente com Auditoria Interna e Controles Internos. Diretoria Financeira: examina e revisa informações relacionadas com o gerenciamento de riscos.

Tabela 7 - Características gerais das políticas e práticas de gerenciamento de riscos de mercado.

Empresa	Detalhes
Ambev	Análise interconectada de riscos financeiros para definição de estratégias. Uso de hedges financeiros. Desde a criação do Comitê de Operações, Finanças e Remuneração da Companhia, a Companhia passou a adotar uma estrutura organizacional de controle de gerenciamento de riscos similar à estrutura e aos controles adotados pela Companhia de Bebidas das Américas – Ambev, promovida por meio de uma infraestrutura integrada que considera o impacto sobre o negócio não apenas de riscos de mercado, mas também de riscos operacionais, estratégicos e de compliance. A política de gerenciamento de riscos abrange quatro pontos principais: (i) estrutura de capital, financiamentos e liquidez; (ii) riscos transacionais relacionados ao negócio; (iii) riscos de conversão de balanços; e (iv) riscos de crédito de contrapartes financeiras.
Petrobras	Conselho de Administração aprova política de riscos da companhia. O ponto de destaque do documento reside em uma abordagem mais abrangente da gestão de risco empresarial, a qual associa a visão econômico-financeira tradicional a elementos de gestão contra ameaças à vida, à saúde e ao meio ambiente (SMES), de proteção do patrimônio e das informações empresariais (Segurança Patrimonial) e de combate à fraude e corrupção (Conformidade Legal), dentre outros riscos empresariais. Há área responsável pelo mapeamento dos processos de gerenciamento de risco via uma matriz de controles. Esta área busca compliance a SoX e responde ao comitê de auditoria. Uso do VaR, testes de estresse e *stops*.
BRF	Aplicação de práticas é de responsabilidade das áreas, apoiados pela Gerência de Riscos, que se reporta ao VP de Finanças e RI. Companhia pratica hedge de câmbio, juros e commodities. A Política de Riscos da Companhia determina limites percentuais a absolutos para exposição de fluxo de caixa em moeda estrangeira, exposição cambial contábil, fluxo de compra de commodities, exposição de consumo a descoberto, exposição de contrapartes financeiras e concentração da carteira de disponibilidades e derivativos, por instituição financeira. Aprovação da política de risco financeiro depende de 2/3 do Conselho de Administração, e a mesma deve conter objetivo do hedge, fatores de riscos, instrumentos limites e alçadas.
Vale	O gerenciamento de riscos pode ser centralizado ou descentralizado dependendo do risco considerado. Monitoramento periódico dos riscos financeiros (câmbio, juros, preços de insumos e produtos). Mitigação dos riscos financeiros via derivativos, levando em consideração o hedge natural. Monitoramento das carteiras consolidadas de derivativos. Práticas incluem monitoramento da execução das políticas de hedge, dos volumes financeiros contratados, do enquadramento de tamanho, necessidade e prazo dos derivativos. O cálculo do valor justo das posições é disponibilizado mensalmente para acompanhamento gerencial.
JBS	Em sua rotina operacional, a Companhia e suas controladas geram exposições diversas a risco de mercado, crédito e liquidez, controladas de maneira integrada pela Diretoria de Controle de Riscos. Riscos financeiros são consolidados pela tesouraria. Uso de VaR e cenários de estresse.

Ultrapar	Busca de casamento cambial, de taxas de juros e uso de derivativos quando necessário. Análise de risco x retorno x liquidez e controle da contabilidade e documentos dos investimentos financeiros.
Embraer	O gerenciamento de riscos da companhia não se limita aos riscos de mercado, incluindo riscos empresariais, operacionais, mercadológicos, de governança e legal. Análise de riscos são feitas com base em entrevistas realizadas com a alta administração, revisões periódicas dos riscos, questionários, reuniões de acompanhamento de Plano de Ação, bem como o endereçamento de ações, validações e avaliações efetuadas pela Alta Administração, sendo reportados ao Conselho de Administração e ao Comitê de Auditoria e Riscos. Uso de planos de ação para cada área de negócio com horizonte de 2 anos, revisados anualmente e atrelados ao plano de ação do CEO. Todos os riscos empresariais possuem seus *Risk Owner*, que reportam e discutem quanto à evolução de cada risco, dos planos de ações de mitigação e indicadores de monitoramento dos riscos. Hedge é contratado com base em custo benefício. Uso do VaR para aplicações financeiras. No uso de *hedge accounting* há documentação do relacionamento entre os itens, e as variações devem se compensar numa faixa de 80 a 125%. A política de gerenciamento de risco da Companhia foi estabelecida pela Diretoria e aprovada pelo Conselho de Administração. O Comitê de Gestão Financeira auxilia a Diretoria Financeira. Nos termos dessa política, os riscos de mercado são protegidos quando não têm contrapartida nas operações da Companhia ou quando é considerado necessário suportar a estratégia corporativa.
Telefônica Brasil	Monitoramento de exposições e uso de derivativos para hedge.
Lojas Renner	Gerenciamento de riscos de forma multidisciplinar, onde a Diretoria avalia se gerenciamento está alinhado com as diretrizes definidas pela Administração. Esta aprova o planejamento anual que pauta a atuação das áreas de Auditoria Interna e de Prevenção de Perdas. Além destes, a companhia conta com uma área de Compliance para alinhar-se às diretrizes dos órgãos reguladores. Derivativos para proteção do risco cambial e da taxa de juros.
CCR	Mitigação dos ricos cambiais, de juros e índice de preço via *swaps plain-vanilla* e NDF. Uso de VaR. Uso de teste de stress.
Kroton	
Eletrobras	Áreas de riscos de subsidiárias conduzem rotinas de controle sob coordenação da holding. Há política de hedge e programa de operações com derivativos. *Hedge* natural e instrumentos não derivativos são prioritários.
Fibria	Os riscos estratégicos são avaliados periodicamente e, em 2014, por meio do processo ERM (*Enterprise Risk Management*), foi identificado que grande parte dos planos de ação estava implementada. Hedge busca diminuir descasamento cambial e volatilidade de fluxo de caixa.A Fibria calcula sua exposição líquida para cada um dos fatores de risco.
Souza Cruz	
Klabin	

Suzano	Processo de gerenciamento de riscos segue o fluxo: identificação e mensuração da exposição; medição dos valores em risco; avaliação de estratégias de gerenciamento; implementação e monitoramento das estratégias. Uso de VaR, testes de estresse e marcação a mercado. De acordo com a política de gestão de riscos de mercado da Companhia, a verificação da adequação das operações da Companhia à referida política deve ser efetuada pelo Consultor ou Analista de Riscos. Caso algum limite seja excedido, cabe ao Consultor ou Analista de Riscos avisar imediatamente e por escrito ao Gerente de Tesouraria, para que este tome as medidas necessárias à readequação dos limites. Se o limite continuar excedido na segunda verificação, que deve ocorrer no dia seguinte, o aviso deve ser dado ao Grupo de Riscos de Mercado. Finalmente, caso o limite continue sendo desrespeitado ao final do terceiro dia, o Consultor de Riscos deve avisar à Diretoria.
Hypermarcas	A Companhia possui e segue uma política de gerenciamento de risco, que orienta em relação a transações e requer a diversificação de transações e contrapartidas. Também são revistos, periodicamente, os limites de crédito e a qualidade do hedge das contrapartes. Nos termos dessa política, os riscos de mercado são protegidos quando é considerado necessário suportar a estratégia corporativa, exposições do fluxo de caixa inferiores a um ano, ou quando é necessário manter o nível de flexibilidade financeira. Uso de mapa de riscos inicialmente feito por consultoria externa e testes de estresse. Desenvolvimento de estudos e monitoramento das condições econômicas e financeiras.

Tabela 8 - Práticas organizacionais de gerenciamento de riscos das empresas nacionais - controles internos e compliance.

Empresa	Detalhes - Controles Internos e Compliance
Ambev	Comitê de Compliance: assessorar o Conselho de Administração nas situações de conflito de interesses em geral, entre a Companhia e partes relacionadas; cumprimento, por parte da Companhia, dos dispositivos legais, regulamentares e estatutários referentes a operações com partes relacionadas e referentes a condutas concorrenciais; outros assuntos que o conselho de administração considerar relevante e no interesse da Companhia. Conselho Fiscal: executa as funções de comitê de auditoria para efeitos da legislação SoX. Deve receber, registrar, processar e examinar reclamações eventualmente recebidas a respeito da contabilidade, controles internos contábeis e assuntos relacionados à auditoria da Companhia, bem como denúncias anônimas recebidas de empregados ou terceiros relacionadas a fraudes contábeis. Diretoria de Auditoria Interna: vinculada ao Conselho de Administração da Companhia, também realiza testes independentes quanto aos controles internos, reportando o seu resultado ao Diretor Presidente da Companhia e ao Comitê de Auditoria. Diretoria alega que de acordo com o COSO os controles internos relativos às demonstrações financeiras não possuem irregularidades.

Petrobras	A companhia disponibiliza para seus funcionários, fornecedores e outras partes interessadas um canal confidencial de denúncias, gerido pela Ouvidoria Geral. Conselho de Administração criou recentemente Área de Governança, Risco e Conformidade (GRC). Sua missão é assegurar a conformidade processual e mitigar riscos nas atividades da companhia, como os de fraude e corrupção. Nova área de GRC deve fortalecer visão integrada dos riscos empresariais, em articulação com as diversas áreas e reportando a diretoria executiva e ao Conselho de Administração, além de cuidar da estruturação da governança e do compliance. Aprovação do Programa Petrobras de Prevenção da Corrupção-PPPC para compliance com a Lei Anticorrupção brasileira. Aprovação do Guia de Conduta da Petrobras, desdobramento pratico do Código de Ética. Aplica-se a membros de conselho, funcionários próprios e há referência ao cumprimento do guia aos prestadores de serviços. Constituição de comitê de correição. Aprimoramento de controles de contratação de serviços de terceiros. Aprimoramento do acompanhamento da execução de projetos. Criação de comitê especial para interlocutor com investigações da Operação Lava Jato. Composto por dois independentes (um estrangeiros) e o diretor de GRC. Controles internos relacionados às demonstrações financeiras são desenvolvidos ou sob a responsabilidade do CEO, Diretor Financeiro ou Comitê de Auditoria.
BRF	Área de controles internos é responsável por acompanhar operações dentro da política de riscos, e é monitorada pela auditoria interna (e auditoria independente). Empresa alega usar o COSO para verificar eficácia de controles internos.
Vale	Diversas áreas atuam como compliance no processo de gestão de risco: a área de *back-office*, integrante da Diretoria Global de Tesouraria e Finanças. Além desta área, a área de controles internos atua para verificar a integridade dos controles que mitigam riscos nas operações contratadas. Conselho Fiscal é responsável por avaliar os controles internos e o sistema de gerenciamento de riscos, de maneira a apurar denúncias, assegurar a sua eficácia e adequação e dos recursos despendidos, qualificação e experiência dos responsáveis e seus programas de treinamento. Cabe ainda ao Conselho Fiscal discutir com o Auditor Externo, Auditoria Interna, Comitê de Controladoria e a Diretoria Executiva de Finanças, o resultado da avaliação do sistema de controles internos como um todo, visando ao seu aprimoramento. Adicionalmente, a auditoria interna também participa no processo de compliance com as normas estabelecidas.
JBS	O Departamento de Auditoria Interna verifica se os processos e as práticas de controle adotadas são adequados e estão funcionando para garantir que os riscos estejam devidamente identificados e controlados O Comitê de Auditoria é responsável por acompanhar recomendações da auditoria interna e externa sobre controles internos, além de avaliar eficiência e qualidade dos controles internos, do compliance e do sistema de gerenciamento de riscos.
Ultrapar	Companhia alega que controles internos sobre demonstrações financeiras possuem compliance com SoX e COSO.

Embraer	Comitê de Auditoria e Riscos: tal comitê também exerce função de comitê de auditoria, garantindo cumprimento da SoX, sendo responsável por monitorar a eficácia dos controles internos, compliance, auditoria e exposições de risco. Auditoria Interna: é responsável por avaliar a suficiência e a eficácia dos controles operacionais e de gestão, verificar a adequação dos processos de identificação e gerenciamento dos riscos e avaliar a eficácia dos controles relacionados à gestão contábil e à geração de relatórios financeiros. Gestão de Riscos e Controles Internos: avalia anualmente os controles internos para atendimento a Lei Sarbanes Oxley Act (SOX) e processos tendo como base os riscos de demonstrações financeiras. Essa avaliação é realizada seguindo o planejamento, walkthrough, Testes de eficácia e Re-teste, caso necessário.
Telefônica Brasil	Controles internos são de responsabilidade do CEO e CFO e avaliados pela auditoria interna. O ambiente de controles internos compreende todos aqueles processos que assegurem razoavelmente o cumprimento de leis, regulações e normas internas, a confiabilidade da informação financeira-contábil, a eficácia e eficiência das operações e a integridade do patrimônio da Companhia. Diretoria avalia que de acordo com o COSO, o sistema de controles internos é adequado.
Lojas Renner	Adequação das práticas das áreas de Auditoria Interna e Prevenção de Perdas ao COSO. Compliance: criada em 2010 para assegurar o alinhamento com as diretrizes dos órgãos reguladores e atuar, principalmente, na prevenção de lavagem de dinheiro, com a área jurídica, que monitora os temas relacionados com normas e legislações vigentes e com a segurança da informação, que atua na prevenção de violação de dados. Outra melhoria instituída no ano de 2014 foi a elaboração da Política Anticorrupção da Lojas Renner, que objetiva explicitar a conduta adotada nos negócios, esclarecer os requisitos gerais da Lei Anticorrupção (Lei 12.846/13) e orientar os colaboradores, parceiros e terceiros sobre a aplicação dos princípios anticorrupção em todas as áreas de atuação da Companhia.
CCR	Comitê de Auditoria: visa a auxiliar o Conselho na definição dos padrões de qualidade dos relatórios financeiros e dos controles internos e, também, avaliar a qualidade dos relatórios financeiros, os riscos envolvidos nos princípios contábeis utilizados e a adequação e eficácia dos controles internos, propondo alterações caso necessário.
Kroton	Comitê de Auditoria: deve definir, juntamente com a Diretoria da Companhia, o escopo de atuação da área de Controles Internos. Temos ainda implantado uma área de Controles Internos que desenvolve testes e trabalhos com o objetivo de aprimorar ainda mais nossos controles.

Eletrobras	Implementação de manual de compliance tendo em vista o FCPA e a Lei Anti Corrupção Brasileira de forma a suprir deficiências apontadas nos controles internos, que incluíram o monitoramento das SPEs detidas pelo grupo e deficiências na elaboração dos relatórios financeiros (especificamente contratos de arrendamento e depósitos judiciais). Criação de gerentes de compliance e uma comissão de compliance. No âmbito de cada empresa, à medida que se demandar apuração de denúncias ocorridas, será instaurada uma Comissão Executiva de Correição. Criação de um programa de comunicação interna. Superintendência de Auditoria, vinculada ao Conselho de Administração, é responsável desde 2011 por verificar adequação e eficácia dos controles internos e o compliance. Empresa alega conformar com o COSO a partir de 2015. Em compliance com a SEC, o CEO e o diretor financeiro avaliam eficácia de controles sobre relatórios financeiros.
Fibria	Auditoria Interna: responsável pela avaliação periódica dos processos financeiros, operacionais, de gestão e de tecnologia da informação, incluindo a sua conformidade com as políticas, normas e procedimentos e o desempenho e a efetividade dos controles internos para prevenir ou detectar a possibilidade de ocorrência de erros, fraudes e/ou perdas no negócio. O Time de Controles Internos continuamente reavalia os fluxos de processos e os sistemas chaves da Organização e garante a realização periódica dos testes de aderência, para aferir a efetividade dos controles existentes como prática da Certificação Contínua – Risk Assessment implementada internamente. Adicionalmente, a Companhia implantou, em 2011, módulo Process Control do GRC SAP, com o objetivo de intensificar a gestão de riscos de processo e compliance, aprimorando e reforçando seu ambiente de controles internos.
Souza Cruz	Auditoria Interna – tem como objetivo principal avaliar a eficácia e integridade dos controles internos, identificar oportunidades de melhoria nos processos e monitorar sua implementação.
Klabin	A Companhia não possui uma política de controles internos aprovada pelo Conselho de Administração. Os mesmos são gerenciados pela área de auditoria interna.
Suzano	Comitê de auditoria é responsável pelos controles internos.
Hypermarcas	O Canal Confidencial também foi repensado e disseminado entre os colaboradores. Tal ferramenta é uma forma de comunicar a Companhia acerca de quaisquer eventos que infrinjam ao Código de Conduta Ética, à Legislação vigente, às políticas, normas e procedimentos internos ou que então sejam inadequados. Sistemas SAP para os controles internos. Diretor Executivo de Controladoria: coordenar procedimentos de auditoria, controles patrimoniais, controles internos e gerenciais da Companhia, responsabilizar-se pela contabilidade da Companhia para atendimento das determinações legais e preparar as demonstrações financeiras da Companhia. Comitê de Ética: formado por colaboradores indicados pela Diretoria Executiva e é responsável pela tomada de decisão em casos de descumprimento das regras estabelecidas, além de ser responsável pela manutenção das ferramentas de gestão da ética. Comitê de Controles Internos: é composto pelas áreas referenciadas nessa parte do relatório e por alguns Diretores Executivos da Companhia, respondendo diretamente ao Diretor Presidente Executivo (CEO). Esse Comitê tem como principais objetivos o alinhamento da

	alta gestão e tomada de decisão referente às atividades dessas áreas. A Equipe de Auditoria Interna tem a responsabilidade de realizar auditoria em processos chave e de suporte ao negócio com o objetivo de adicionar valor a partir da aplicação de uma abordagem sistêmica e disciplinada para avaliar a eficácia dos processos, controles e governança.

Tabela 9 - Práticas organizacionais de gerenciamento de riscos das empresas nacionais - riscos distintos de riscos de mercado.

Empresa	Detalhes
Ambev	Há uma infraestrutura integrada que considera o impacto sobre o negócio não apenas de riscos de mercado, mas também de riscos operacionais, estratégicos e de compliance. Há ferramentas e políticas de metas visando a mitigação de risco ambiental, tais como monitoramento dos gases de efeito estufa e redução da geração de resíduos sólidos em seus processos.
Petrobras	Não há seguro para as pausas nas operações no Brasil, especialmente as devido a greve, sabotagem ou guerra. Não há hedge de commodities, exceto proteção dos resultados esperados de transações comerciais de curto prazo. Há Comitê Ambiental formado por membros do conselho de administração para lidar com meio ambiente e segurança ocupacional. Uso de políticas e diretrizes corporativas, investimentos em centros de proteção ambiental e prevenção de desastres ambientais, obtenção de certificações. Metas de maximização de eficiência energética.
BRF	Mitigação de risco climático: gerenciamento de estoque, eficiência energética.
Vale	Uso do ISSO31000 no gerenciamento dos riscos operacionais. A gestão de seguros é realizada com o apoio dos comitês gerenciais de seguros existentes nas diversas áreas operacionais da Companhia.
JBS	Gastos com tratamento de resíduos para mitigação de risco ambiental. Mitigação de riscos socioambientais via reuso de resíduos, manutenção preventiva de equipamentos, treinamento de funcionários, mecanismos de contrato com fornecedores e investimentos em tecnologia. Mitigação de risco de fechamento de mercados de exportação via diversificação internacional das operações.

Ultrapar	Mitigação do risco ambiental via certificações de segurança, meio ambiente e saúde, além de ampliação do uso de matérias primas renováveis e afiliação em 2010 à mesa-redonda da produção sustentável de óleo de palmiste (insumo de uma das controladas).
Embraer	Provisões para risco de pedido de troca de aeronave vendida. Projetos de mitigação de risco de desaceleração de vendas e lucratividade, visando custos menores e produtos de melhor qualidade. Monitoramento do risco do sistema de financiamento do mercado de aeronaves. Cooperação com entidades para garantir acompanhamento tecnológico. Diversificação de fornecedores e e clientes. Monitoramento da saúde financeira de ambos e da competitividade dos produtos. Monitoramento geral de exposições financeiras e de exigências contratuais de pilotos. Existência de equipe de gestão de crise de produto. Mitigação de riscos ambientais via política própria, consultoria externa e sistemas para garantir compliance. Obtenção de certificações de saúde e segurança ocupacional.
Telefônica Brasil	
Lojas Renner	Contratação de seguros conforme as práticas usuais de mercado; seguro de responsabilidade civil geral para se proteger de eventual sinistro. Mitigação do risco de inaugurar novas lojas. Dentre as ações incluem-se estudos de inteligência de mercado, relacionamento com empreendedores de shoppings e desenvolvimento de alternativas estratégicas de canais de venda. Mitigação do risco de ineficiência (sobrecarga) operacional Ações envolvem planejamento de TI, centros de distribuição e programas de sucessão gerencial. Mitigação do risco de vendas decrescentes. Iniciativas culturais dentro da corporação, inovações financeiras, inovações em novos canais de vendas e padronização de processos. Mitigação do risco de não atender as demandas dos consumidores. Uso de monitoramento das preferências dos consumidores e gestão de fornecedores. Mitigação do risco de perda de margem financeira. Contratos de curto prazo e diversificação de fornecedores. Mitigação de práticas irregulares na cadeia de fornecedores. Área de gestão de fornecedores, auditoria e monitoramento de fornecedores e programas de certificação.
CCR	
Kroton	Reajuste da principal receita (mensalidades) de acordo com a inflação.
Eletrobras	Além de seguros, a Eletrobras Eletronuclear atendeu a todas as solicitações feitas pelo CNEN relacionadas à avaliação das lições aprendidas em razão do acidente em Fukushima, incluindo a realização de "testes de estresse" desenvolvidos para as usinas nucleares europeias seguindo as diretrizes estabelecidas pela Comissão Europeia.
Fibria	Provisão própria de fontes renováveis complementada com fontes não renováveis para mitigar riscos de falta de energia. Implementação dos Comitês de Gestão de Crises e realização de simulados. Monitoramento do preço da celulose. Não existe hedge em função do mercado pouco desenvolvido para esta commodity.

Souza Cruz	Grupo com estratégias anti-comércio ilegal e participação em fóruns de ética concorrencial para mitigar o risco do comércio ilegal. Monitoramento de tendências regulatórias e monitoramento de tendências legais para minimizar risco de indenizações. Investimentos em segurança para mitigar roubo de carga. Programa de continuidade de negócio para planos de contingência e gestão de crises. Apoio técnico a cadeia de fornecedores para prevenir falta de abastecimento. Certificações de meio ambiente, saúde ocupacional e segurança para cumprimento de normas ambientais.
Klabin	Contratação de seguros para unidades industriais e transportes. Não contratação de seguros para áreas florestais, devido a condições especificas da sua localização geográfica e em função da natureza de suas atividades, da distribuição das florestas em diversas áreas distintas e das medidas preventivas adotadas contra incêndio.
Suzano	Fixação de parte da exposição aos preços de commodities que façam parte de sua cadeia produtiva, como petróleo e celulose. Investimentos em certificações, no monitoramento e conservação de recursos naturais para mitigar risco ambiental.
Hypermarcas	Sistema de gestão ambiental e monitoramento de indicadores ambientais com base em melhores práticas. Processo de qualificação e avaliação de fornecedores de serviços ambientais.