

Compliance

RISK ASSESSMENT


em 8 passos

POR BRUNO PIRES BANDAROVSKY

COMPLIANCE RISK ASSESSMENT (CRA)


OU MAPEAMENTO DE RISCOS DE COMPLIANCE, é reconhecido mundialmente como um dos requisitos de validade e eficácia de um Programa de Compliance. É considerado também, pelos Chief Compliance Officers e demais profissionais da área, como um dos processos mais complexos do Compliance Corporativo, gerando grandes preocupações e, até mesmo, chegando a tirar o sono de muitos de nós. Mas, seria este processo realmente um bicho-papão? Mesmo sendo complexo, será que podemos torná-lo mais palatável, sem comprometer a sua eficácia e adequando-o às nossas rotinas?

**POR BRUNO PIRES
BANDAROVSKY ***



Neste e-book, pretendo, simplificadamente, nivelar conceitos, explicar a sua importância sob a ótica das normas internacionais, abordar métodos de planejamento e execução, na tentativa de desmistificar essa “fera”, tornando-a domável e amigável para melhor servir a vocês e possibilitar aprimoramento contínuo de seus Programas de Compliance.

Inicialmente, como advogado que sou, mencionarei bases legais relevantes para ilustrar a obrigatoriedade de adoção do CRA. Prometo ser rápido, limitando o “juridiquês” a poucos parágrafos.



** Bruno Pires Bandarovsky é Sócio de Rolim, Viotti & Leite Campos Advogados, membro da Society of Corporate Compliance and Ethics (SCCE), membro do Comitê de Ética e da Comissão de Combate à Corrupção na Causa da ABDIB, membro do GT Integridade do Instituto Ethos, membro do GT Anticorrupção da Rede Brasil do Pacto Global da ONU, membro do Instituto Compliance Brasil, membro da Comissão de Estudos Permanentes de Compliance do IASP, membro do Instituto Não Aceito Corrupção, Chief Compliance Officer terceirizado do Grupo Promon.*



“A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT”

No âmbito da regulamentação da legislação dos EUA sobre as práticas de corrupção realizadas no exterior por entes sujeitos à jurisdição dos EUA, (*Foreign Corrupt Practices Act - FCPA*), o *Department of Justice (DoJ)* e a *Securities and Exchange Commission (SEC)* co-publicaram, em novembro de 2012, um documento chamado “*A Resource Guide to the U.S. Foreign Corrupt Practices Act*”.

Seu capítulo 5 contém uma seção que trata especificamente das características essenciais de Programas de Compliance efetivos. Dentre estas, encontra-se o CRA. Seus editores fizeram questão de evidenciar que Programas de Compliance não são oferecidos nas vitrines, em “tamanho único”, sendo indispensável que cada organização conheça adequadamente os riscos aos quais está exposta e adote mecanismos de mitigação proporcionais à relevância destes.

Por sua vez, em respeito ao artigo 9º da norma anticorrupção do Reino Unido (*United Kingdom Bribery Act - UKBA*), o Ministério da Justiça daquele país publicou, em março de 2011, dois documentos de orientação relevantes – “*Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing*” e “*Quick start guide*”.

Com relação ao primeiro, no capítulo intitulado “*The six principles*”, são descritos seis procedimentos básicos que devem formar o conjunto de estratégias de uma organização para a prevenção de eventos de corrupção. O terceiro deles é o CRA.

O documento estipula que a organização deve mapear a natureza e

a extensão de sua exposição a potenciais riscos externos e internos de corrupção praticada por indivíduos atuando em seu nome, determinando, ainda, que tal mapeamento deve ser realizado periodicamente, ser objeto de comunicações internas e ser adequadamente documentado.

NO BRASIL



No Brasil, o Decreto nº 8.420/15 regulamentou a Lei Anticorrupção Brasileira ou Lei da Empresa Limpa (Lei nº 12.846/13). No inciso V, do artigo 18, o decreto estabelece que a existência de um Programa de Integridade instituído conforme o que está descrito no Capítulo IV da mesma norma poderá ensejar uma redução da pena de multa resultante da condenação em um Processo Administrativo de Responsabilização (PAR). Tal redução pode se dar na proporção de 1% a 4% do faturamento da empresa no exercício anterior ao da instauração do processo, a depender do grau de consistência verificada no referido Programa de Integridade. Por sua vez, no citado Capítulo IV, mais especificamente no inciso V do artigo 42, determina-se como requisito de validade e eficácia a “análise periódica de riscos para realizar adaptações necessárias ao programa de integridade”.

AGORA, CONFORME O PROMETIDO, CHEGA DE “JURIDIQUÊS”!

Já deu para perceber que não há conformidade sem CRA, concorda?
Então, por que é necessário fazê-lo?
Por que preciso fazê-lo periodicamente?
Não posso mesmo me livrar desse negócio complicado de uma única vez?

Da mesma forma que não há dois indivíduos iguais, cada organização é um ente único. Pode haver duas parecidas, mas ao conhecê-las melhor, logo verificaremos a existência de diferentes culturas organizacionais, estruturas corporativas, líderes, processos operacionais, abordagens mercadológicas, cadeias de fornecimentos, enfim, uma multiplicidade quase inesgotável de fatores que as tornam únicas, inigualáveis. Assim, duas organizações muito semelhantes até poderiam ter Programas de Integridade semelhantes, contudo jamais seriam idênticos ou cegamente replicados.

A forma adequada para descobrir, evidenciar e tratar essas especificidades de cada organização, as quais podem se materializar em riscos de Compliance, é o processo de Mapeamento de Riscos de Compliance.

E não sou eu quem está dizendo – são as normas internacionais, baseadas nos conceitos e procedimentos reconhecidamente eficazes referentes ao tema Gestão de Riscos.

COM BASE NOS RISCOS DE COMPLIANCE IDENTIFICADOS NO PROCESSO DE CRA, É POSSÍVEL:

- ✓ Criticar a eficácia
- ✓ Adequação
- ✓ Atualidade do arcabouço normativo de Compliance das empresas
Código de Conduta, Políticas, Procedimentos, cláusulas contratuais
- ✓ Ajustar os controles internos voltados para a mitigação dos riscos ou instituir novos
- ✓ Identificar a necessidade de fortalecer a comunicação interna ou as sessões de treinamento em determinados aspectos
- ✓ Propor modificações em processos operacionais
- ✓ Ajustar o tom adotado pela liderança



O CRA, planejado e executado por meio dos métodos recomendados, provê ao Compliance Officer uma ferramenta de trabalho poderosa, voltada para o aprimoramento de seu Programa, em todos os seus pilares. Ele permite a adoção de uma estratégia de evolução consistente, em vez de basear-se apenas na sensibilidade e experiência dos profissionais da área.

O CRA PRECISA SER EXECUTADO PERIODICAMENTE

A flexibilidade em estabelecer a periodicidade em que o processo de CRA será executado precisa ser um atributo do Compliance Officer e da alta liderança, avaliando o grau, a velocidade e o alcance de cada movimento de mudança de uma organização.

Como sabemos, também, se há um processo inesgotável na vida das pessoas e das empresas, este é a mudança. Nada é estático em nosso mundo. A economia mundial, integrada como está, e a rapidez e alta permeabilidade da informação impõem às organizações a necessidade de ler os movimentos de mercado e responder a eles com agilidade, num processo adaptativo constante, que resulta em mudança contínua – sob pena de insucesso ou até descontinuidade. Vocês reconhecem isso em suas vidas e em suas empresas? Pois este processo de mudança contínua promove, igualmente, mudança contínua nos panoramas de riscos das organizações, motivo pelo qual o CRA precisa ser executado periodicamente,

De todo modo, parece eficaz rodar ciclos, ao menos, de 3 em 3 anos (reflita com base no histórico dos últimos 10 anos de sua organização)

sob pena de apodrecimento de seu Programa de Compliance.

Quanto a tal periodicidade, propositalmente, não há regras que a definam. Por mais que determinada empresa tenha convencionado que executará ciclos bienais, determinada mudança, em meio tempo, poderá sugerir a execução de um ciclo extemporâneo - seja envolvendo toda a organização ou, por exemplo, apenas uma unidade de negócios ou um processo operacional.

Este é o momento no qual recorro a um dos conceitos que ficaram muito marcados em minha mente, em decorrência das aulas da cadeira de Estratégia Empresarial, no MBA de Gestão Empresarial, que fiz na década passada: ***jacaré que dorme vira bolsa!*** Perfeitamente aplicável, não?

EXPERIMENTE “DORMIR” SEM TOCAR NO SEU PROCESSO DE CRA QUE, MAIS DIA MENOS DIA, DAS DUAS UMA: OU UM ENTE EXTERNO DESQUALIFICARÁ SEU PROGRAMA DE COMPLIANCE, OU A PROBABILIDADE DE OCORRÊNCIA DE UM EVENTO INDESEJÁVEL AUMENTARÁ, SEM QUE VOCÊ SEQUER O PERCEBA. CONVÉM EVITAR.

Bem, parece-me que, neste momento, compreendemos para que serve o CRA, por que precisamos dele e por que necessitamos executá-lo periodicamente. Vamos falar de metodologia? Para isso, primeiramente, vou tratar de alguns conceitos. Não me limitarei aos significados encontrados em dicionários, pois vou adaptá-los à realidade do tema.

RISCOS

São ameaças aos valores de uma organização, sejam estes econômicos, reputacionais, legais ou regulatórios, mercadológicos ou operacionais.

Por sua vez,

FATORES DE RISCO são eventos que podem desencadear a materialização de um risco. Como exemplo, podemos afirmar que a eventual interação de determinados profissionais da empresa com autoridades públicas é um fator que pode materializar o risco de corrupção.

No CRA, o que se pretende é identificar os riscos de Compliance aos quais a empresa está exposta, quais os fatores de risco existentes, qual o impacto potencial na organização e a probabilidade de materialização, quais as medidas mitigatórias já existentes, quais devem ser aprimoradas ou adicionadas (bem como quais devem ser suprimidas!), qual o plano de implantação dos ajustes às medidas mitigatórias e como este será monitorado pela Unidade de Compliance.



Nossa, parece complicado mesmo, não é? A vida do profissional de Compliance já é tão corrida, como viabilizar a realização de um processo desses? É quando me recordo de outro conceito valioso das aulas de Estratégia Empresarial: ***se você precisa abraçar um gorila, não encare o bicho inteiro; primeiro fatie o gorila e depois pegue fatia por fatia!*** No nosso caso, a resposta é **MÉTODO** e **PLANEJAMENTO**.

Em relação ao método, não vamos reinventar a roda, e sim aprender com quem sabe e dedicou tempo de estudo suficiente para estabelecer melhores práticas.

COSO

Por este motivo, destaco o *Committee of Sponsoring Organizations of the Treadway Commission (COSO®)*, uma organização sem fins lucrativos, criada nos EUA em 1985, dedicada a melhoria dos relatórios financeiros, sobretudo pela aplicação da ética e efetividade na aplicação e cumprimento dos controles internos. É patrocinado por cinco das principais associações de classe de profissionais ligados à área financeira nos EUA. Em decorrência da globalização e padronização internacional das técnicas de auditoria, as recomendações da COSO, relativas aos controles internos, bem como seu cumprimento e observância, são amplamente praticados e tidos como modelo e referência no Brasil e na maioria dos países do mundo.

No site da COSO, é possível efetuar o download gratuito de diversos materiais de valiosa aplicação nas empresas. Dentre eles, para fins de estruturação de um ciclo de CRA, destaco “Risk Assessment in Practice”, com apenas 19 páginas. Obviamente, é apenas uma compilação dos principais aspectos da metodologia, mas já ajuda bastante. Se for do seu interesse, é possível adquirir o material completo via web, a preço simbólico. A seguir, pincelarei a estrutura metodológica de um bom CRA, criado com base na metodologia da COSO, combinada com a metodologia PDCA, criada pelo Dr. W. Edwards Deming.



FONTE: WWW.COSO.ORG

PASSO Nº ZERO

CONHEÇA SUA ORGANIZAÇÃO

O número é zero porque sem isso não há estrutura de CRA válida, nem possibilidade de ação como Compliance Officer em uma organização. Se você é novo na empresa, é indispensável que faça uma imersão para conhecer sua cultura, sua história, o que pensa a liderança, o que a empresa faz (e como o faz), qual o perfil dos colaboradores, clientes e fornecedores, quais riscos já se materializaram, qual o histórico de casos trazidos à ouvidoria ou canal de denúncias, qual a realidade do mercado no qual a empresa atua, dentre os diversos elementos estratégicos e ambientais cujo conhecimento é fundamental.

PASSO Nº 1

CONHEÇA SUA JURISDIÇÃO

Avalie as normas às quais a sua organização está submetida e às quais precisa demonstrar atendimento.

Vou dar um exemplo simples: a sua empresa pode ser brasileira e estar submetida unicamente às normas brasileiras relativas a temas de Compliance. Contudo, devido à atividade desempenhada, pode ser exigido de sua empresa, por clientes multinacionais, a completa aderência a normas de outros países, como o FCPA, podendo tal exigência tornar-se, até mesmo, um *deal breaker*.

Por isso, estude essas normas e veja quais os comportamentos proibidos e aqueles que são exigidos ou desejáveis, bem como as sanções aplicáveis - sua grade de

riscos e fatores de riscos no CRA deverá, sem dúvida, considerá-los.

Se sua empresa já possui um Código de Ética, saiba que esta norma interna deve ser igualmente considerada para identificar riscos e fatores de risco para o exercício. Outras fontes, como, por exemplo, os manuais da CGU ou até mesmo literatura específica, podem ser considerados como fontes para este mesmo fim.

PASSO Nº 2

MONTE A GRADE DE RISCOS E FATORES DE RISCO

Compilando as fontes identificadas no passo anterior, verifique os riscos e fatores de risco convergentes, montando uma grade única que contemple todas as fontes, em todas as jurisdições a serem consideradas. Numere, sequencialmente, todos os fatores de risco, de forma a poder identificá-los facilmente no futuro, podendo acessá-los apenas pela numeração conferida a cada um.

FATOR DE RISCO - FR <i>(FR = como o risco se materializa)</i>	Grupo de Risco ?	Impacto Probabilidade Inerente
Prometer, oferecer, dar, receber, direta ou indiretamente, vantagem indevida , por meio de refeição, brinde, presente, entretenimento ou hospitalidade , a agente público ou privado , ou a terceira pessoa a ele relacionada (relação de parentesco ou relacionamento pessoal).	Corrupção	3-Moderado 4-Alta

PASSO N° 3

CRIE A MATRIZ DE IMPACTO E PROBABILIDADE

AVALIAÇÃO DE IMPACTO

Com base na realidade de sua empresa, você deverá conceituar e classificar o impacto:

IRRELEVANTE

LEVE

MODERADO

SEVERO

CATASTRÓFICO

Desejavelmente, essa classificação deve ser feita quantitativa e qualitativamente (use uma coluna para cada).

POR EXEMPLO:

Para determinada organização o impacto pode ser considerado leve se, sob o aspecto quantitativo, causar incômodo sem efeitos perenes, com aplicação de multas e/ou redução de receitas gerando comprometimento do fluxo de caixa, com impacto de até 5% do faturamento ou do patrimônio líquido. Já, do ponto de vista qualitativo, pode considerar a aplicação de sanções, podendo haver menção midiática pontual, com pequeno a médio potencial de dano à imagem.

Por outro lado, a definição de impacto catastrófico da mesma organização poderia indicar, sob o aspecto quantitativo, o comprometimento significativo da continuidade da empresa através da aplicação de multas e/ou redução de receitas gerando comprometimento insolúvel do fluxo de caixa, conduzindo para processos de concordata/falências, e prejuízo continuado superior a 40% do custo de manutenção das atividades. Já sob o aspecto qualitativo, poderia indicar a declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos da punição; percepção de inidoneidade disseminada no mercado (perda de inúmeras oportunidades de negócio); condenação criminal de algum profissional envolvido.

EXEMPLO DE MATRIZ DE AVALIAÇÃO DE IMPACTO

IMPACTO POTENCIAL – GRADUAÇÃO		
	QUALITATIVA	QUANTITATIVA
1 - INSIGNIFICANTE	Aplicação de sanções de baixa relevância, sem efeito midiático nem de imagem.	Impacto irrelevante - aplicação de multas e/ou redução de receitas gerando comprometimento irrelevante do fluxo de caixa. Impacto de até 0,5% do faturamento ou do patrimônio líquido.
2 - LEVE	Aplicação de sanções, podendo haver menção midiática pontual, com pequeno a médio potencial de dano à imagem.	Causa incômodo, sem efeitos perenes - aplicação de multas e/ou redução de receitas gerando comprometimento do fluxo de caixa. Impacto de até 5% do faturamento ou do patrimônio líquido.
3 - MODERADO	Aplicação de sanções relevantes, com menção midiática relevante e dano à reputação causando empecilhos à concretização de negócios.	Gera preocupação importante com o rumo do negócio - aplicação de multas e/ou redução de receitas gerando comprometimento razoável do fluxo de caixa e resultado em pelo menos 1 exercício.
4 - SEVERO	Suspensão temporária de participação em licitações públicas; impedimento de contratar com órgãos da Administração Pública; menção midiática relevante e recorrente, com dano à reputação que dificulta ou impede a concretização de negócios.	Tira o sono dos executivos/acionistas e gera perda relevante - aplicação de multas e/ou redução de receitas gerando comprometimento relevante do fluxo de caixa. Prejuízo de até 30% do custo de manutenção das atividades em pelo menos 2 exercícios.
5 - CATASTRÓFICO	Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos da punição; percepção de inidoneidade disseminada no mercado (perda de inúmeras oportunidades de negócio); condenação criminal de algum profissional envolvido;	Compromete significativamente a continuidade da empresa - aplicação de multas e /ou redução de receitas gerando comprometimento insolúvel do fluxo de caixa, conduzindo para processos de concordata/falências. Prejuízo continuado superior a 40% do custo de manutenção das atividades.

AValiação DE PROBABILIDADE

Ainda, com base na realidade de sua empresa, você deverá conceituar e classificar a probabilidade de materialização do risco (muito baixa, baixa, média, alta e muito alta). Por exemplo, em uma organização a probabilidade pode ser considerada muito baixa se quantitativa-

vamente prever-se uma ocorrência em 100 mil e qualitativamente ser considerada quase nula. Por outro lado, a probabilidade pode ser considerada alta, se quantitativamente prever-se uma ocorrência em 100; e, qualitativamente ser considerada possível.

EXEMPLO DE MATRIZ DE AVALIAÇÃO DE PROBABILIDADE

PROBABILIDADE DE OCORRÊNCIA - GRADUAÇÃO		
<i>INERENTE = Comportamento da empresa com base em sua cultura RESIDUAL = cultura + controles existentes TARGET = Residual + controles desejáveis/necessários</i>	QUALITATIVA	QUANTITATIVA – MERAMENTE EXEMPLIFICATIVO
1 - MUITO BAIXA	QUASE NULA	Qtde de ocorrências - Ex: 1 em 100 mil
2 - BAIXA	REMOTA	Qtde de ocorrências - Ex: 1 em 10 mil
3 - MÉDIA	Depende da ocorrência concomitante de um conjunto de fatores POSSÍVEIS ou PROVÁVEIS	Qtde de ocorrências - Ex: 1 em 1 mil
4 - ALTA	POSSÍVEL	Qtde de ocorrências - Ex: 1 em 100
5 - MUITO ALTA	PROVÁVEL	Qtde de ocorrências - Ex: 1 em 10

Naturalmente, essa matriz deve ser discutida com a liderança da empresa, antes de se rodar o ciclo de CRA, com o objetivo de alinhamento de percepções e critérios, bem como para viabilizar uma adoção oficial de métricas para avaliação dos riscos na empresa.

PASSO Nº 4

CLASSIFIQUE TODOS OS FATORES DE RISCO DE SUA ORGANIZAÇÃO COM BASE NO GRAU DE RISCO INERENTE

O grau de risco inerente é aquele ao qual a organização está naturalmente exposta, desconsiderando todos os controles mitigatórios já existentes na organização. Sugere-se considerar apenas a cultura da organização e o ambiente no qual ela está inserida para o exercício de suas atividades. Assim, avalie impacto e probabilidade de materialização de cada fator de risco, com base na matriz definida no passo anterior. Em seguida, situe visualmente a numeração de cada fator de risco em um gráfico no qual, no eixo x, sejam criados 5 quadrantes para impacto (de irrelevante a catastrófico); e, no eixo y, 5 quadrantes para probabilidade (de muito baixa a muito alta).

EXEMPLO DE MATRIZ DE AVALIAÇÃO DE PROBABILIDADE

Probabilidade	5 Muito Alta	4 Alta	3 Média	2 Baixa	1 Muito Baixa	Insignificante	Leve	Moderado	Severo	Catastrófico
						1	2	3	4	5
			34					11	16	
								5 12 19 20 31 42	2 3 4 6 7 8 14 17 18 21 24 26 36	35
								13 22 29 30 32 33 37 38 41 43 44 45 46	9 10 25 27 28 39	15
									23 40	1

Após posicionar todos os seus fatores de risco nesse gráfico, você terá uma representação visual do **RISCO INERENTE** de Compliance da sua organização.

PASSO Nº 5

PLANEJE AS SUAS ENTREVISTAS

Identifique os *process owners* das diversas áreas de sua organização e relacione com quais fatores de risco eles estão expostos.

Assim, você identificará quantas entrevistas precisará realizar e quais os temas que precisarão ser abordados na entrevista com cada área da organização.

Vale a pena avaliar a realização de sessões de entrevistas envolvendo, ao menos, duas áreas simultaneamente. Mas avalie cuidadosamente.

Por um lado, entrevistas individuais, por área, projetam um número total maior de entrevistas.

Por outro lado, entrevistas com áreas diferentes, acontecendo simultaneamente, podem ser extensas e gerar a sensação de perda de tempo aos participantes no momento em que particularidades de uma determinada área estejam sendo discutidas.

PASSO N° 6

REALIZAÇÃO DAS ENTREVISTAS

Nessas entrevistas, os *process owners* deverão criticar a classificação do risco inerente e apontar as medidas mitigatórias já existentes na organização para cada fator de risco, caso elas já existam.

Desta forma, deverá ser acordada entre entrevistador e entrevistado, uma classificação de impacto e probabilidade para o grau de **RISCO RESIDUAL** ou **ATUAL**, ou seja, o grau de risco ao qual sua organização está exposta considerando o conjunto de medidas e controles mitigatórios atualmente em prática.

Situe, visualmente, a numeração de cada fator de risco em um novo gráfico, à semelhança do gráfico realizado para Risco Inerente, no passo 4.

Desta vez, aloque-os de acordo com a avaliação do Risco Residual.

FORMAS DE TRATAMENTO

Neste momento, do ponto de vista metodológico formal é necessário avaliar, juntamente com os *process owners*, a estratégia de tratamento a ser considerada para cada risco, com base em sua natureza e sua classificação na matriz de Risco Residual. Há quatro formas de tratamento: evitar, reduzir, transferir/compartilhar e aceitar.

Em termos mais simples e práticos, avalie se os fatores de risco na matriz de Risco Residual já se encontram situados numa posição que possa ser considerada como nível desejável para sua organização. Caso essa posição não traga o conforto necessário, nessa mesma entrevista deverão ser discutidos e acordados o aprimoramento das medidas existentes ou a instituição de novas, com o objetivo de levar o risco em análise a um patamar desejável.

EVITAR

Este é um tratamento de exclusão. É o caso de um risco muito acentuado e de difícil, impossível ou estrategicamente indesejável mitigação. Neste caso, decide-se por interromper a atividade que materializa o fator de risco analisado.

REDUZIR

Neste caso é encontrada uma estratégia viável econômica e operacionalmente para reduzir impacto e/ou probabilidade, como meio de mitigação do risco analisado. Resulta num plano de ação acordado entre os *process owners* e a equipe que está executando o CRA.

TRANSFERIR / COMPARTILHAR

É aplicável para situações em que o meio de mitigação do risco analisado é a transferência ou o compartilhamento do mesmo com terceiros. É o caso clássico da contratação de uma apólice de seguros ou a contratação de um transporte de valores por empresa de segurança como meio de mitigar o risco de roubo de valores.

ACEITAR

Ocorre quando a classificação de um risco na matriz de Risco Residual já se encontra em padrões desejáveis ou aceitáveis, ou ainda quando as ações de mitigação identificadas não sejam viáveis ou recomendáveis numa avaliação da relação entre o custo da ação pretendida com o benefício de sua implantação (relação custo/benefício).

LEMBRE-SE QUE AS MEDIDAS PRECISAM SER PROPORCIONAIS AOS RISCOS, NÃO FAZENDO SENTIDO ALGUM PROPOR UM APRIMORAMENTO ALTAMENTE CUSTOSO PARA UM RISCO COM O QUAL A EMPRESA POSSA CONVIVER DE UMA FORMA MINIMAMENTE SAUDÁVEL.

Por fim, acorde com este process owner o plano de implantação deste aprimoramento ou da nova medida, bem como qual a forma pela qual a Unidade de Compliance obterá evidência ou, minimamente, indicação de que o plano de ação está sendo cumprido com êxito.

PASSO Nº 7

MONTE UMA MATRIZ COM O GRAU DE RISCO DESEJÁVEL OU TARGET

Com base nas entrevistas realizadas, crie uma matriz que represente, graficamente, o impacto e a probabilidade desejáveis para cada risco, situando os fatores de risco nos quadrantes para os quais devam se mover após a conclusão do plano de ações acordado com cada *process owner*.

Ao situar, lado a lado, as 3 matrizes, com os graus de risco **INERENTE**, **RESIDUAL** e **DESEJÁVEL**, respectivamente, você terá, visualmente, a adequada identificação do status atual de sua organização em relação aos riscos de Compliance e vislumbrar para quais níveis de risco a organização será levada com a adoção dos ajustes operacionais ou estratégicos desenhados.

EXEMPLO COMPARATIVO ENTRE MATRIZES DE RISCO INERENTE, RESIDUAL E TARGET



Níveis de Tratamento
A = Adoção imediata de estratégias de proteção e prevenção
B = Reflexão sobre adoção de ações de curto/médio prazo ou monitoramento de forma rotineira e sistemática
C = Monitoramento de forma rotineira e sistemática, podendo incluir planos de emergência
D = Risco em Zona de Conforto

Níveis de Tratamento
A = Adoção imediata de estratégias de proteção e prevenção
B = Reflexão sobre adoção de ações de curto/médio prazo ou monitoramento de forma rotineira e sistemática
C = Monitoramento de forma rotineira e sistemática, podendo incluir planos de emergência
D = Risco em Zona de Conforto

Níveis de Tratamento
A = Adoção imediata de estratégias de proteção e prevenção
B = Reflexão sobre adoção de ações de curto/médio prazo ou monitoramento de forma rotineira e sistemática
C = Monitoramento de forma rotineira e sistemática, podendo incluir planos de emergência
D = Risco em Zona de Conforto

PASSO Nº 8

MONITORE A IMPLANTAÇÃO DOS AJUSTES ÀS MEDIDAS MITIGATÓRIAS

Tenha um *cockpit* em suas mãos pelo qual você consiga identificar e controlar se os passos acordados estão sendo efetivamente adotados e no tempo acordado.

Importante lembrar que as mais diversas medidas mitigatórias podem surgir do processo de CRA. Desde ajustes no ERP de sua organização e reestruturações de áreas, ajustes

nos processos entre as diversas áreas da organização, criação ou adaptação de treinamentos, campanhas de comunicação interna ou externa, mudanças em seu Código de Conduta, suas políticas e procedimentos e até mesmo mudanças de pessoas ou da estratégia da organização. As possibilidades são infinitas.



Ah, claro! Lembre-se que tudo deve ser documentado. Registre atas das reuniões realizadas, inclusive entrevistas. Registre, periodicamente, o avanço de cada passo. Crie *track record*, crie evidência de seu processo de CRA.”

Existem algumas formas de “fatiar esse gorila”. No seu caso, pode ser interessante realizar o processo aos poucos, de forma continuada. Por exemplo, comece pelos riscos inerentes mais graves em sua matriz. Você, provavelmente, terá menos entrevistas e entrevistas menores, portanto, será mais econômico e atingirá primeiro o que precisa ser priorizado. Mas, lembre-se que, para isso, deverá ter passado pelos passos 1 a 4, fazendo esta avaliação no passo 5. Assim, poderá planejar suas ações de forma continuada, ao longo de dois ou três anos, estabelecendo esta como a periodicidade a ser adotada.

Outra forma de fatiar o processo são reuniões por áreas de risco - desde que as características de sua organização acarretem na concentração de riscos mais graves em determinados entes organizacionais. Igualmente ao que descrevemos acima, nesse caso, a execução do ciclo será continuada, começando pelo que é prioritário e, em seguida, cumprindo o processo nas áreas menos críticas.

Outro ponto muito relevante: lembre-se que jamais o Compliance Officer de uma organização deve se isolar da alta liderança.

Ele é o motorista do processo de Compliance da empresa, mas o dono do caminhão é o time de liderança. Não trafegue com este veículo sem o devido acompanhamento do dono. É vital que os critérios de avaliação, a abrangência dos riscos e dos fatores de risco, a priorização do plano de execução do CRA, os resultados, o plano de ação acordado com os *process owners*, bem como o acompanhamento da implantação deste plano sejam compartilhados e suportados pela alta liderança, conforme os níveis de governança de cada organização. E não esqueçam de criar e aproveitar oportunidades para reforçar o *Tone at the Top*, divulgando comunicados da alta liderança sobre o processo de CRA.

**Como fazer isso tudo?
Ninguém melhor que você
para estabelecer esse plano
com base no conhecimento
de seus líderes e da governança
de sua organização.**

Chegando ao final do e-book, quero lembrá-los que, em nenhum momento, eu afirmei que um processo de CRA bem feito é simples. Tentei desmitificá-lo e torná-lo mais tangível. Não é simples. Mas, faça-o, inexoravelmente, faça-o, se necessário com o apoio de especialistas – para sua proteção e de sua organização.

A propósito, se for do seu interesse, estou à disposição para conversar mais com você a respeito deste ou de outros assuntos – procurem-me, por meio do e-mail b.bandarovsky@rolimvlc.com.



CONTATO

+55 11 3259-2837
CONTATO@LECNEWS.COM



ENDEREÇO

AV. PAULISTA, 1274 - 120 ANDAR, CONJ. 32
ED. ASAHI - BELA VISTA - SÃO PAULO / SP

WWW.LECNEWS.COM