

A high-angle, blurred photograph of a crowd of people walking on a light-colored floor with a hexagonal tile pattern. The image is tinted with a light blue and green color scheme.

Boas Práticas para o Uso Estratégico de Controles Internos

Apresentação	2
I. Planejamento das matrizes de risco e controle.....	3
II. Construção da estrutura de controles e aplicação do RCSA.....	13
III. Ações de melhoria da estrutura de controle.....	18
IV. Anexo I – Parametrizando a matriz de controle na prática	20

Otimize sua estrutura de controles

Apresentação

O presente artigo reúne o conjunto de melhores práticas observadas ao longo das experiências dos consultores da ELO Group em projetos de gestão de risco operacional e controles internos para empresas nacionais e multinacionais.

De forma objetiva, estas melhores práticas devem ser entendidas pelo leitor como *insights*, aprendidos ao longo dos projetos realizados, que impactam significativamente no resultado de ações de construção e manutenção de estruturas controles internos.

Tais melhores práticas incluem o planejamento prévio de ações, construção das matrizes de risco e elaboração de planos de ações, devendo apoiar substancialmente organizações que estejam nos mais distintos estágios de implantação da estrutura de controles internos, maximizando seu valor percebido e otimizando o esforço necessário.

Finalmente, observa-se que os projetos analisados possuíram os mais distintos objetivos desde simples aplicações do método de RCSA (*risk control self-assessment*), passando por atendimento a resolução 3380/Basiléia II (específico para instituições financeiras), até casos de adequação as seções 302 e 404 da SOX (específico para empresas de capital aberto na bolsa de Nova York).

I - Planejamento das matrizes de risco e controle

1. Definir claramente o que está sendo entendido por “risco”, explicitando possíveis confusões com outras referências

Para minimizar o re-trabalho e evitar erros de comunicação dentro da empresa é essencial que se delimite o que está sendo entendido por risco. No que diz respeito às matrizes de risco, esse entendimento será um fator chave para o seu desenvolvimento.

Um exemplo de definição é a proposta da IIA (Institute of Internal Auditors) que considera o risco como “*qualquer coisa que possa impedir o alcance dos objetivos*”. Essa definição é normalmente utilizada em abordagens de RCSA.

Outro exemplo de definição para risco baseado na futura norma ISO 31.000, seria “*efeito da incerteza nos objetivos*”. Nesse caso, cabe ressaltar que tanto incertezas que impactam os resultados da organização negativamente quanto positivamente são considerados pela norma.

Em ambos os casos o risco é entendido como um conjunto de diversos componentes, incluindo *causa* (fontes de risco ou vulnerabilidades, existentes na organização, que podem dar origem a um evento), *evento* (contexto ou situação em que a perda ou ganho ocorre) e *conseqüências* (diferentes tipos de perdas causadas pelo evento).

Essa descrição ampla do risco permite entender como os *controles* poderiam atuar: (1) minimizando a probabilidade das *causas* efetivamente provocarem o *evento*, ou, (2) minimizando o impacto das *conseqüências* dado que o *evento* já ocorreu.

Outra abordagem é dada pela aplicação dos conceitos de risco operacional nas instituições financeiras. Essas, direcionadas pela Basileia, tendem a interpretar o risco operacional como “*a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos*”.

Além disto, neste segmento é muito comum que os profissionais associem diretamente o risco aos eventos de risco operacional listados pela Basileia II/Resolução 3380 (fraudes internas; fraudes externas; práticas inadequadas com clientes; etc).

Passando para empresas sujeitas à SOX, observa-se uma tendência ao entendimento dos riscos como eventos que levem a perda de confiabilidade ou credibilidade de um determinado *report* ou divulgação financeira. Formalmente, um risco operacional relativo a *report* financeiro pode ser definido como: *“um evento ou condição que pode afetar negativamente a habilidade de uma determinada organização de produzir relatórios financeiros de uma maneira tempestiva e confiável.”*

Na prática, para projetos de adequação as seções 302 e 404 da SOX, o risco operacional é tratado como um evento ou um conjunto de eventos indesejados que possam ocorrer na preparação e divulgação de relatórios financeiros. Em particular, estes eventos indesejados representam erros em contas que possuem materialidade para a organização e que possam ferir um conjunto de assertivas realizadas pela gestão da empresa, como ocorrência e existência, completude/integridade; alocação e mensuração, direitos e obrigações e apresentação e divulgação.

Em suma, é fundamental que a organização defina claramente o que será entendido por risco em sua ação de gestão de controles internos, apoiando a utilização de diversos instrumentos de trabalho, entre eles, a matriz de risco.

Uma última ressalva é relativa ao perigo de se considerar o risco como qualquer coisa que possa interferir no atingimento de um objetivo. Embora a definição de risco esteja relacionada aos objetivos, associar qualquer coisa que impacte nestes não é necessário, e torna o trabalho menos eficiente. Ao invés de contemplar qualquer coisa que poderia dar errado, a identificação dos riscos deve ser direcionada pela compreensão de eventos inesperados, ocorridos na prática da operação e que impactem no atendimento dos objetivos. Isso permite a restrição do escopo da análise; focando-a sobre os problemas reais da operação.

Eventos de baixíssima probabilidade, como catástrofes climáticas, pandemias, etc, não são foco de atenção específico em um CSA, sendo melhor analisados em técnicas de maior poder preditivo, como a análise de cenários. Desta forma, o conteúdo do CSA deve ser direcionado pelo que efetivamente dá errado na organização e não por qualquer coisa que poderia dar errado.

2. Planejar com cautela quais serão os instrumentos utilizados para criação e validação das matrizes de riscos e controles

Dos métodos usados para criação da estrutura de controles internos, três são mais freqüentemente abordados pela literatura: questionários; entrevistas e workshops. Como era de se esperar, a decisão pela utilização de cada um desses métodos irá depender das particularidades de cada empresa e de cada projeto. Contudo, sugerimos a utilização de um híbrido destes três métodos, para geração de resultados mais completos, rápidos e efetivos.

- **Questionário** – ideal para a coleta extensiva e rápida de informação. Podem ser utilizados para um diagnóstico relativamente superficial da estrutura de controles e/ou quando a empresa possui informações suficientemente estruturadas sobre riscos; controles e objetivos. Outra forte indicação para o seu uso é no momento de priorização de processos a serem avaliados (podendo inclusive restringir a análise mais detalhada dos processos mais críticos). Finalmente, trata-se de uma ferramenta interessante para monitorar mudanças na estrutura de controles já mapeada (revisão das matrizes de risco)
- **Entrevistas** – ferramenta indicada para o primeiro levantamento da estrutura de controles internos de uma empresa, já que permite a interação entre quem detêm o método da construção da matriz de risco (consultores externos ou áreas específicas da organização) e quem possui o conhecimento profundo da operação (executores e gerentes). Sua aplicação demanda mais tempo do que os questionários, mas produz informações significativamente mais detalhadas. Entrevistas costumam ser feitas em duas etapas: uma primeira entrevista de levantamento e uma segunda de validação. Cabe ressaltar que o levantamento extensivo de controles existentes, realizado através de entrevistas, deve seguir um padrão para o registro e detalhamento das informações, permitindo a geração de um relatório final homogêneo e uma análise da viabilidade para manutenção da base de dados gerada.
- **Workshops** – ferramentas indicadas para situações que exigem decisões importantes e a participação de múltiplos *stakeholders* com tempo disponível limitado, como gerentes e diretores. *Workshops* são ideais para dois momentos: primeiro, no momento de identificação dos objetivos e principais riscos no início da ação; e, segundo, para validação do resultado geral de uma

ação de controles internos, na qual planos de ação e respostas de tratamento aos riscos são aprovados e priorizados.

3. Definir um dicionário de riscos que efetivamente possa ser utilizado como linguagem única da organização

Uma primeira definição, crucial para o bom andamento do processo, é a formalização do dicionário de riscos (ou universo de riscos). Ele deve descrever todas as categorias de risco às quais a organização está exposta. Categorias de risco comuns são: riscos operacionais, riscos de mercado; riscos de crédito; riscos de *underwriting*, riscos de liquidez, risco estratégico, etc.

Em muitos casos, faz-se necessário o detalhamento de categorias de riscos operacionais em subcategorias, de modo a refletir os eventos de risco operacional que realmente podem ocorrer em uma organização. Exemplos desses detalhamentos são as categorias de fraudes, demandas trabalhistas, etc. para a Basiléia e as categorias relacionadas às assertivas das contas materiais existentes nos relatórios financeiros (existência e ocorrência, completude/integração, avaliação e alocação, direitos e obrigações e apresentação e divulgação para SOX)

A definição de um dicionário de risco é importante por duas razões. Por um lado, a definição do dicionário garante a robustez no levantamento de riscos, assegurando que todos os riscos pertinentes à empresa serão mapeados. Por outro lado, se bem aplicada, ela ajuda a gerenciar o esforço da organização ao garantir que a construção das matrizes de risco está focada nos problemas centrais da empresa.

4. Planejar anteriormente quais atributos devem ser utilizados para avaliar os riscos

Outra questão chave para a criação da estrutura de controles internos é a definição dos atributos a serem avaliados para cada um dos riscos operacionais. Certos atributos podem, por exemplo, ser avaliados em relação a escalas (como alto, médio e baixo), outros serão avaliados através da classificação dos riscos em diferentes categorias (como pessoa, processo ou sistema). As classificações mais utilizadas para risco são:

- **Risco inerente x Risco residual:** Uma decisão importante está em optar por uma avaliação separada dos riscos em relação ao “risco inerente” e “risco

residual”. De maneira prática, avaliar o risco inerente significa avaliar a probabilidade e severidade da ocorrência de um risco, desconsiderando-se a estrutura de controles atual. A avaliação de risco residual é análoga, exceto por considerar a existência da estrutura de controles atual.

A realização de ambas as avaliações é indicada quando se deseja medir a efetividade da estrutura de controles, já que esta é exatamente a diferença entre o risco inerente e residual. Além disso, a análise do risco inerente e residual promove uma compreensão da eficiência da estrutura de controles permitindo a identificação de possíveis excessos na estrutura de controles internos (por exemplo, se existem muitos controles para mitigar um risco que inerentemente já é baixo).

Vale ressaltar, entretanto, que esta distinção não é um consenso entre as normas e muitas organizações possuem grandes dificuldades em avaliar o que seria risco inerente, pois não conseguem visualizar sua operação sem os controles existentes.

- **Código de referência** – Um outro *insight* prático importante é a criação de códigos de referência para os riscos identificados. A criação destes códigos, associados ao dicionário de risco, permite a realização de consultas e *queries* por risco nas matrizes de risco. Isso se mostra particularmente relevante porque as matrizes de risco são normalmente feitas por processo, e muitos riscos aparecem em mais de um processo (e, portanto mais de uma matriz).

5. Planejar anteriormente quais escalas de severidade e probabilidade serão utilizadas

Na prática, grande parte das empresas se utiliza de três dimensões ou parâmetros para a avaliação de um risco. A primeira delas é a probabilidade de uma determinada fonte de risco gerar um evento, ou a probabilidade de um determinado evento de risco ocorrer. A segunda é a severidade de suas conseqüências, dado que um evento de risco ocorreu. E a terceira é uma escala que consolida os parâmetros de severidade e probabilidade em um só parâmetro (alto, médio ou baixo, por exemplo), o que possibilita a comparação entre diversos riscos de forma mais direta. A decisão de que

escalas utilizar é importante, pois deve estar alinhada a exposição real ao risco da organização e ao seu apetite ao risco.

Um ponto importante a ser ressaltado é que avaliar os riscos de acordo com escalas permite compara-los entre si. Para isso é necessário definir quais propriedades serão avaliadas através dessas escalas.

A probabilidade de um evento de risco ocorrer está normalmente ligada à complexidade, subjetividade e necessidade de julgamento das atividades de cada processo. Além disso, a probabilidade de cada risco ocorrer guarda forte relação com a efetividade dos controles preventivos (controles preventivos e detectivos serão abordados posteriormente neste documento). A correlação entre riscos é outro fator que afeta a probabilidade de um determinado risco ocorrer de maneira significativa. Na prática, as empresas adotam escalas de 3 ou 5 níveis associadas à probabilidades (10%; 20%; 30% de chance de ocorrência; etc) ou à frequências de ocorrências (1 vez por dia; 1 vez por semana, 1 vez por mês; etc).

Já a severidade de um evento de risco operacional costuma depender do volume de transações de cada processo e do montante de dinheiro movimentado por este. Na prática, as empresas adotam escalas de severidade em diversas dimensões: impacto financeiro (escala de valor monetário), impacto na reputação (escalas de clientes impactados ou quantidade de divulgação do evento de risco), escalas de segurança (número de mortes ou ferimentos), etc.

A prática mostra que a utilização de diversas dimensões nas escalas de severidade pode trazer um retrato mais fidedigno da importância dos riscos para a organização. Entretanto, a utilização de muitas dimensões tende a complexificar significativamente a análise, tornando-a mais difícil, demorada e, conseqüentemente, onerosa.

Outro *insight* importante é referente a construção de uma avaliação para o risco, dado uma determinada probabilidade e severidade. Este instrumento unificado de avaliação é interessante, pois facilita a ordenação dos riscos em listas e sua comunicação para a organização. Entretanto, deve-se ter especial atenção quanto a classificação dos riscos que possuem alta severidade e baixa probabilidade, bem como os riscos de baixa severidade e alta probabilidade.

Estes dois tipos de riscos representam *trade-offs* entre dimensões de severidade e probabilidade, e por isso devem ser analisados de forma distinta. Para instituições

financeiras em particular, riscos de alta severidade e baixa probabilidade tendem a ser classificados como altos, pois estes dominam o cálculo de seu capital econômico alocado. Já riscos de alta probabilidade e baixa severidade, tendem a ser classificados como médios, pois são naturalmente mais perceptíveis e normalmente possuem uma quantidade razoável de controles associados.

6. Planejar com antecedência quais atributos devem ser utilizados para analisar os controles

De forma análoga ao que foi comentado para o risco operacional, deve-se definir quais atributos serão utilizados para classificar os controles possuídos pela organização e como essa caracterização será feita (em escalas, qualificações, etc.). Na prática, essas classificações auxiliam no entendimento de diversas propriedades de controle, apoiando discussões de priorização de ações de melhoria e análises de *gaps* de controle. As classificações mais utilizadas de controle são:

- **Controle manual x Controle automático** – Uma operação suportada por sistemas mais robustos de TI (como pacotes prontos ou ERPs) está sujeita a falhas nos sistemas, falta de disponibilidade ou erros lógicos dentro do sistema. Já uma operação mais manual é exposta a erros de informações, falta de disponibilidade de dados, etc. Dessa forma, a classificação do controle em manual e automático facilita o entendimento de como as deficiências de controle podem impactar a operação, apoiando assim o projeto de testes de controles e a avaliação de possíveis *gaps* da operação.
- **Detectivo, preventivo e compensatório** – Um controle preventivo tende a agir sobre a probabilidade de ocorrência de um determinado evento, impedindo que este aconteça. Já um controle detectivo visa mitigar a severidade de um evento já ocorrido. Um controle compensatório tende a existir para contrabalançar uma falha na estrutura de controles, impedindo que eventos de risco ocorram, ou diminuindo sua severidade.

Esta classificação facilita distinguir se um determinado controle atua sobre a probabilidade da ocorrência de um evento de risco ou sobre a severidade da mesma. O uso de controles compensatórios também se mostra uma opção interessante para firmas menores que desejam diminuir o custo da estrutura de controles. Desta maneira, uma análise interessante da estrutura de

controles pode ser realizada através da categorização de controles associada à avaliação dos riscos existentes.

Primário e secundário – Um controle primário é aquele que é constituído das atividades ou tarefas realizadas que são particularmente críticas para a mitigação do risco associado. Controles primários provêm garantia razoável de que os objetivos da operação serão atingidos, através da redução do risco de um resultado indesejado a um nível aceitável. Além disso, esses controles são confiáveis do ponto de vista de seu *design* e efetividade.

Já controles secundários são controles que não são considerados tão importantes em relação a sua contribuição para a mitigação do risco em questão. Muitas vezes estes controles não são totalmente confiáveis do ponto de vista de seu *design* e efetividade, sendo frequentemente associados a controles compensatórios.

A identificação dos controles que melhor mitigam cada risco é importante para a priorização de *gaps*, deficiências e melhorias da estrutura de controle, assim, como para agilizar processos de testes e de auditoria de controles. Em uma ação de melhoria da estrutura de controles internos, por exemplo, filtrar a análise da população de controles para uma amostra de controles críticos é essencial para garantir resultados rápidos e de baixo custo.

- **Periodicidade** – essa classificação visa explicitar que os diversos controles existentes para mitigar um determinado risco podem estar sendo executados muitas vezes em tempos diferentes.
- **Código de referência** – de forma análoga aos riscos, um código de referência para cada controle é importante para habilitar *queries* e consultas na estrutura de controles. Como um controle normalmente mitiga mais de um risco, *queries* de riscos mitigados por controle podem ser muito úteis ao se considerar uma alteração na estrutura de controle.

7. Planejar como considerar as questões de compliance interno e externo

A adequação com normas e órgãos reguladores é uma preocupação tão relevante para as empresas que o COSO criou uma categoria de objetivos relacionados

exclusivamente a riscos de não *compliance* com normas e órgãos reguladores existentes.

Muitas vezes, no ambiente de rápida mudança em que às empresas se inserem, o risco de não adequação com normas reguladoras está associado a não aderência a políticas; procedimentos e manuais internos de operação ou à padrões técnicos de referência (como padrões ISO; *British Standards*, etc). Com isso, pode-se replicar o conceito de *compliance* com normas e órgãos reguladores para entender que o *compliance* deve acontecer também internamente.

Desta forma, as matrizes de risco devem apontar os itens de *compliance* externo (regulações, normas e leis) e *compliance* interno (procedimentos; manuais; políticas e normas técnicas) relacionados a cada item identificado. Isso permite o entendimento de como cada evento de risco pode implicar também em um evento de não *compliance*.

Em alguns casos, podem surgir dúvidas técnicas como: “Um procedimento deve ser considerado um controle ou como um documento que grupa um conjunto de controles a serem realizados?” Para resolver estes problemas, é fundamental a associação do procedimento ao risco envolvido, podendo-se assim entender o grau de granularidade/detalhamento necessário.

8. Definir claramente como as responsabilidades serão delegadas entre risk owner, control owner e process owner

A discussão da gestão de riscos traz a tona uma pergunta interessante, que muitas vezes não era abordada de forma sistemática e estruturada nas organizações: quem dentro da organização é responsável por um determinado risco operacional – quem é o *risk owner*?

O significado do que seria um *risk owner* pode ser melhor compreendido abordando a idéia da criação de um representante da organização que é responsável pela avaliação do risco e pela definição da suficiência e robustez do conjunto de controles existente na mitigação de um risco de forma satisfatória.

Contudo, a aplicação prática do conceito de *risk owner* revela uma grande restrição: como convencer um determinado *risk owner* a aceitar a responsabilidade pela gestão de uma série de controles que provavelmente estão fora de sua área funcional de ascendência gerencial?

Não há dúvidas que todo *risk owner* inevitavelmente acaba sendo um funcionário (com certo nível hierárquico) responsável por gerenciar a grande maioria dos controles que mitigam um determinado risco em questão. Entretanto, como lidar com os controles presentes em outros processos e em outras áreas funcionais sem causar desconforto ou conflitos? Este problema tende a se agravar na medida em que os *risk owners* se constituem em uma posição de responsabilidade com baixo grau de autoridade associado.

De forma a materializar esta discussão, sugerimos algumas soluções distintas para esse problema, como pode-se ser observado abaixo. Importante ressaltar que ambas as sugestões podem ser utilizadas de forma híbrida, customizando a ação de gestão de riscos para as características das áreas e processos da organização.

- Definição do *risk owner* como alguém que efetivamente tem a visão completa do processo atravessando todas as áreas funcionais. Estes *risk owners* devem possuir autoridade formal e documentada para que de fato tenham algum mecanismo para acompanhamento, cobrança e punição da correta execução dos controles nas diversas funções em que o risco está associado.
- Definição do *risk owner* como alguém que avalia se o conjunto de controles existente é o mais eficiente possível para mitigação do risco, sendo responsável apenas por mobilizar a organização para este determinado fim. Contudo, a análise da confiabilidade de cada controle, assim como cobrança para sua manutenção, execução e melhoria fica distribuída em cada uma das áreas que o risco abrange.
- Não existe a figura do *risk owner*. A análise da conformidade e eficiência do conjunto de controles para mitigação de um determinado risco deve ser definida colaborativamente pelos gestores das áreas envolvidas neste processo.

Construção da estrutura de controles e aplicação do RCSA

9. Analisar a estrutura de controles internos por uma lente de riscos

Recentes manuais e normalizações que fazem referência a adoção de práticas de controles internos vêm recomendando uma abordagem orientada a riscos. Desta forma, a quantidade de esforço empregado por uma determinada organização para construção e manutenção de uma estrutura de controles internos (leia-se mapeamento de processos, documentação de controles e construção de matrizes de risco) deve estar alinhada a uma avaliação prévia dos riscos enfrentados por esta organização.

Um risco mais significativo exige controles mais formais e processos mais detalhados, que produzam evidências expressivas de sua adoção. Já riscos com menor relevância podem ser mitigados por controles mais tácitos e menos precisos, exigindo um menor esforço de documentação e explicitação de evidências.

10. Adequar a estrutura de controles à organização, e não a organização à estrutura de controles

O impacto de exigências de controles internos em organizações de menor porte tende a ser maior do que nas organizações de maior porte. Por exemplo, um comitê de auditoria que custe 100 mil reais ao ano poderia onerar significativamente o orçamento de uma empresa que fatura 100 milhões de reais, no entanto, o mesmo não ocorreria em uma que faturasse 1 bilhão. Além disso, empresas maiores podem fazer uso de economias de escala em seus controles usando, por exemplo, procedimentos e políticas mais formalizados e sistemas mais robustos.

A estrutura de controles deve se adequar a organização, e não o contrário. A estrutura de controles internos não deve ser um fardo, mas um instrumento de gestão poderoso.

11. Analisar os riscos em controles nas diversas camadas da organização

Muitas vezes, empresas orientam a análise de seus controles internos somente aos seus processos, pois nestes reside o maior trabalho e os controles mais facilmente identificáveis. No entanto, é necessário analisar os controles que atuam em

determinadas áreas da empresa (ou nela toda) e não necessariamente na execução dos processos. Essa análise focada em áreas específicas é chamada pelo COSO de *Entity Assessment* e pode ser realizada através de um questionário.

A importância deste *assessment* está no fato de que, muitas vezes, uma deficiência de controles internos de um processo pode ser suprida por um controle existente na área que o executa. Um determinado processo pode, por exemplo, não ter controles anti-fraude suficientemente bons, mas se a gerência onde for executado possuir bons instrumentos de punição e um bom código de ética (controles da entidade), o risco de fraude pode se mostrar tratado de forma suficiente.

12. Entender a estrutura de controles como um todo e não como componentes separados

O entendimento e avaliação de uma estrutura de controles devem ser realizados de forma holística e integrada. O foco deve ser avaliar se um conjunto de controles mitiga os riscos existentes adequadamente ou não.

Por diversas vezes ainda é válida a discussão da eficiência de um determinado conjunto de controles. Ou seja, mesmo que um conjunto mitigue inteiramente um determinado risco, é possível que um outro conjunto de controles o possa fazê-lo a um custo menor? Ou, será que algum dos controles existentes é excessivo, podendo ser descontinuado sem que se altere significativamente o risco residual?

13. Aplicar benchmarkings internos para alavancar a estrutura de controles

Muitas vezes, ótimas soluções de controle existentes dentro da organização, por não serem devidamente reconhecidas, acabam subutilizadas. O entendimento da estrutura de controles habilita a descoberta de excelentes soluções dentro da empresa permitindo a replicação destas para outras áreas, processos, produtos e serviços.

Além disto, deve-se sempre ter em mente a possibilidade de maximizar o número de riscos mitigados por um determinado controle, otimizando assim os ganhos gerados por sua execução.

14. Utilizar controles compensatórios, sempre que aplicável, para reduzir o custo da estrutura de controles

Muitas vezes uma empresa não tem condições de implementar a estrutura de controles desejada. Controles de segregação de atividades, por exemplo, geram altos custos por incharem a folha de pagamento devido à criação de novos postos de trabalho.

Controles compensatórios podem ser uma boa saída para minimizar este custo. Em um processo de fechamento contábil, por exemplo, uma empresa pode não contar com múltiplos executores, mas realizar uma análise amostral do processo e uma conciliação, substituindo, de maneira efetiva, o controle de segregação de atividades.

15. Otimizar, sempre que possível, o esforço no mapeamento dos controles

Alguns *insights* importantes da prática podem levar a uma otimização do esforço de mapeamento dos controles e construção das matrizes de risco:

- Não é necessário detalhar riscos não significativos. Uma boa prática é agregar riscos até obter uma significância razoável. Na prática isso significa que riscos excessivamente pequenos podem ser agregados para entrar de forma mais significativa na análise. Excesso de detalhe eleva muito o custo de manutenção da documentação associada.
- Não é necessário descrever dois riscos que possuem conjuntos de controles associados idênticos. Agregar esses riscos em uma mesma descrição é uma boa saída para evitar redundâncias na matriz de risco.
- É importante avaliar sempre o custo benefício da construção de matrizes de riscos distintas para produtos ou serviços muito semelhantes. Embora a orientação pela redução de esforço sempre possível seja importante, juntar riscos com controles associados sensivelmente diferentes pode distorcer a análise.
- Por fim, recomenda-se o descarte de riscos irrelevantes para a empresa, que na prática só implicam em um aumento do custo de manutenção das matrizes de risco. A chave para tanto está em fazer matrizes focadas nos problemas da operação.

16. Não confundir riscos com ausência de controles ou com o não atingimento de objetivos

Outro desafio encontrado na prática é a própria descrição de cada risco. Alguns erros mais comuns são descrever o risco como a ausência de controles ou o risco como o inverso de um objetivo:

- **Risco como ausências de controles** – o risco não pode ser um não controle. Como regra genérica, risco deve representar o problema e o controle a solução. Dessa forma a ausência de uma determinada solução não pode se constituir em um problema, até porque, na grande maioria das vezes, existem mais de uma solução possível para o mesmo problema. Por exemplo, para o processo de faturamento de produto, a “ausência de segregação de atividades” não é um risco, mas o “faturamento de um produto que não possui nota fiscal” é.
- **Riscos como não atingimento de objetivos** – o risco também não pode ser descrito como a negação de um objetivo. Se um objetivo da operação é “obter 95% de satisfação de clientes”, um risco não pode ser descrito como “não obter 95% de satisfação de clientes” ou “obter um índice de satisfação de clientes abaixo de 95%”. A descrição do risco deve prover *insights* sobre o que pode dar errado na operação, sobre que tipos de eventos podem levar ao não atendimento do objetivo. No exemplo anterior, poderíamos escrever alguns riscos como “perda de dados relativos a clientes”; “entrega de produtos fora do prazo ou fora de conformidade com as especificações” ou “violação de níveis de serviço acordados”.

17. Não deixar de mapear as EUC (End User Computing) Tools utilizadas, como tabelas em Access e planilhas em Excel

Um fator de risco importante para a grande maioria das empresas é a quantidade de informações críticas presentes em aplicativos e sistemas pessoais que apresentam um baixo grau de confiabilidade de dados e de modelos lógicos de processamento. Um bom *insight* da prática é mapear todas as planilhas Excel, base de dados em Access e sistemas legados que contém informações cruciais para a empresa. Esse mapeamento é uma importante fonte de informação para analisar as vulnerabilidades de TI e os *gaps* existentes na estrutura de controles.

18. Atentar para os direcionadores que alertem para uma expectativa de mudança na exposição ao risco

Outro desafio que necessita de atenção é a mudança do nível de exposição a risco de cada processo. Na prática, alguns direcionadores podem fazer com que um processo cujos riscos estiveram sob controle durante muito tempo, passe a ter uma nível de exposição acima do desejado, mesmos sem o aparecimento de novos riscos. Alguns sinais podem alertar para alterações significativas no nível de exposição a risco de um determinado processo e, conseqüentemente, na efetividade de sua estrutura de controles internos:

- Mudanças recentes no processo;
- Alterações no volume de transação;
- Alterações em características específicas de processos rotineiros (manuais, políticas e procedimentos), características de processos de fim de período (frequência e método) e pressupostos existentes (regras de negócios, estimativas, etc).
- Influência de fatores externos (taxas de câmbio, competidores, ambiente regulatório, etc.)
- Alterações representativas na força de trabalho disponível existente ou nas condições de trabalho dos funcionários atuais.

Ações de melhoria da estrutura de controle

19. Compreender a diferença entre possuir o controle e poder demonstrá-lo

Muitas vezes a necessidade de se demonstrar a existência de um controle através de documentos, históricos e evidências, onera mais a organização do que o próprio controle. Para o COSO, existem três níveis de formalização, em ordem crescente: (1) aquele que satisfaz a gerência/diretoria para conduzir o negócio; (2) aquele que é necessário para que a diretoria se responsabilize formalmente pelos erros na operação e (3) aquele necessário para que a companhia possa ser auditada.

Entender os objetivos da estrutura de controle e definir o grau de formalização necessário para cada risco é fundamental para uma implantação eficiente de uma estrutura de controles internos.

20. Tratar erros de design e erros de implementação de forma diferenciada

Erros na estrutura de controle devem ser analisados contra critérios de (1) adequação do design ou projeto e (2) adequação da implementação. Tais critérios geram decisões diferentes em relação à melhoria da estrutura de controles.

Notadamente, uma falha de design indica a necessidade de adição e/ou substituição de controles, e uma falha de implementação indica a necessidade de aprimoramento da execução e reforço de mecanismos de monitoramento.

21. Desenvolva um processo sistêmico de documentação e revisão da estrutura de controles internos

A estrutura de controles não deve ser abordada apenas por um projeto isolado. Ela deve estar ligada a um processo que ajude a organização a entender os riscos de sua operação e mitigá-los de maneira satisfatória. Para tal, um processo sistêmico e periódico de documentação e revisão de controles deve ser estabelecido.

Vale lembrar que os mecanismos que acionarão a revisão de controles podem variar de acordo com os processos. Diversas alternativas podem ser consideradas como: ocorrências de perdas, revisão anual, mudanças em processos ou tecnologias, etc.

22. Planejar antecipadamente como os planos de ação deliberados serão geridos

A gestão dos planos de ação para tratamento de riscos e *gaps* na estrutura de controle deve priorizá-los de acordo com a probabilidade e severidade de cada risco e com a agenda das áreas internas. Muitas vezes, planos de ação acabam sobrecarregando diversas áreas que não possuem a capacidade ou o orçamento para realização de todas as ações desejadas. Tal fato tende a ocorrer fortemente nas áreas de suporte das empresas, como por exemplo, a área de Tecnologia da informação, que tende a receber muitas demandas de automatizações e desenvolvimento de funcionalidades.

Alguns pontos devem ser ressaltados nesse sentido:

- **Considere a capacidade das áreas internas em relação à complexidade da ação** - entenda claramente qual a complexidade de cada ação, os atores envolvidos e as restrições orçamentárias e de capacidade interna das áreas, para priorizar adequadamente estas ações. Como mencionado acima, é ilusório designar diversos pontos de melhoria para TI ou processos sem, no entanto, definir devidamente quais serão as prioridades de forma real, baseando-se no orçamento e na disponibilidade de pessoal capacitado.
- **Definição de responsáveis por plano de ação** – sem uma definição clara de responsabilidades (e de quem cobra o responsável), os planos de ação podem cair em vácuos de responsabilidade ou na rotina, levando a sua não implantação adequada. Pode ser interessante definir uma lógica de classificação entre planos de ação por sua abrangência (se o plano de ação é funcional ou corporativo) e uma lógica de prioridade, baseado em critérios objetivos e alinhados aos desejos do corpo de diretores e do conselho de administração da empresa.
- **Outras considerações relevantes** – considere a ligação dos planos de ação com outros mecanismos próprios, como sistema de qualidade, business plan, planejamento estático, etc.

Anexo I – Parametrizando a matriz de controle na prática

Um desafio bastante prático e que muitas organizações enfrentam é a parametrização da matriz de controle, ou seja, decidir quais colunas devem existir em uma determinada matriz para que esta atenda as necessidades da organização.

De uma maneira geral, esse desafio foi abordado ao longo deste documento, aonde foram discutidas todas as possibilidades de parametrizações da matriz. Desta forma, o objetivo deste anexo é prover ao leitor um resumo breve das decisões que necessitam ser tomadas para a parametrização de uma matriz de risco na condução do RCSA. Este resumo pode ser encontrado na tabela abaixo, que sumariza as principais decisões a serem tomadas. Estas decisões ainda foram alocadas em uma matriz de risco genérica (na seqüência) para facilitar sua visualização.

Checklist para matrizes de controle
a) Qual será a classificação dos riscos (quanto aos fatores de risco, eventos ou consequência)?
b) Haverá classificação de controles entre automático e manual?
c) Haverá classificação de controles entre detectivo e preventivo?
d) Haverá uma avaliação de controles contra design e execução?
e) Haverá uma classificação de controle como primário e secundário?
f) A periodicidade de execução de cada controle será avaliada?
g) O risco residual será avaliado?
h) Haverá avaliação dos riscos será feita de acordo com o conceito de risco inerente?
i) Quais serão as escalas de severidade e probabilidade utilizadas?
j) Quem avalia cada risco (executor, gerente, diretor, grupo de trabalho, etc)?
k) Serão modelados os riscos para os objetivos de eficiência operacional, de compliance e de report financeiro?
l) Haverá discussão de formas de tratamento de risco?
m) Haverá a discussão de plano de ação para riscos não mitigados/controles insuficientes?
n) Haverá a explicitação do control owner?
o) Haverá a explicitação do risk owner?

Objetivo	Risco	Risk Owner	Avaliação do risco inerente			Controle	Control Owner	Categoria de controle	Tipo de controle	Primário/Secundário	Frequência do controle	Efetividade Design	Efetividade Operação	Avaliação do risco residual			Mecanismo de tratamento	Plano de ação
			Probabilidade	Severidade	Consolidado									Probabilidade	Severidade	Consolidado		
Objetivo 1	Risco 1	Gerente X	Baixo	Baixo	Baixo	controle A	Executor X	Preventivo	Automático	Primário	Constante	Suficiente	Suficiente	Baixo	Baixo	Baixo	NA	NA
	Risco 2	Executor Y	Médio	Médio	Alto	controle B	Executor Y	Preventivo	Automático	Primário	Mensal	Suficiente	Suficiente	Baixo	Médio	Médio	NA	NA
						controle D	Executor Z	Detectivo	Manual	Primário	Diário	Suficiente	Suficiente	Baixo	Médio	Médio	NA	NA
	Risco 3	Gerente W	Alto	Alto	Alto	controle E	Executor X	Detectivo	Manual	Primário	Semanal	Insuficiente	Insuficiente	Alto	Alto	Alto	Compartilhar	Plano de ação 1
Objetivo 2	Risco 6	Gerente W	Médio	Baixo	Médio	controle A	Executor Z	Detectivo	Manual	Secundário	Constante	Razoável	Suficiente	Baixo	Baixo	Baixo	Compartilhar	Plano de ação 1
	Risco 7	Executor Z	Alto	Alto	Alto	controle F	Gerente N	Detectivo	Automático	Primário	Constante	Razoável	Suficiente	Baixo	Baixo	Baixo	Compartilhar	Plano de ação 1
						controle G	Executor Z	Preventivo	Manual	Primário	Diário	Razoável	Insuficiente	Médio	Médio	Médio	Diminuir severidade	Plano de ação 3