4
Estabelecimento e hierarquização de regras de monitoramento contínuo: proposta metodológica

Este capítulo tem por objetivo apresentar uma metodologia para estabelecer e hierarquizar regras de monitoramento no âmbito de um projeto de auditoria contínua de uma empresa do setor elétrico brasileiro. Mais especificamente, a metodologia compreende a seleção dos processos auditáveis com maior exposição ao risco; a identificação de eventos de risco associados a esses processos; o estabelecimento de regras para monitoramento e auditoria contínua; e a hierarquização propriamente dita das regras de monitoramento segundo cinco critérios, a saber: (i) cumprimento de regras estabelecidas pela Aneel; (ii) verificação do cumprimento de metas de qualidade no atendimento aos consumidores; (iii) redução de perdas elétricas e financeiras; (iv) avaliação de controles que tenham o objetivo de mitigar a ocorrência de erros ou fraudes; (v) cumprimento de exigências legais de outros órgãos.

No contexto atual de gestão de riscos e controles internos nas empresas, uma estratégia que vem sendo amplamente utilizada é a de implantar ou aprimorar os controles internos com base na identificação e mensuração dos riscos empresariais. É possível considerar a existência de duas abordagens de mensuração de riscos – a qualitativa e a quantitativa.

Pela abordagem qualitativa, o nível de risco é avaliado a partir da atribuição de critérios de classificação à probabilidade de ocorrência e ao impacto (impacto financeiro e outros).

Uma das técnicas empregadas para avaliação qualitativa de riscos é o processo de auto-avaliação conhecido como *Control Self Assessment* (CSA), que consiste em avaliar, de maneira descentralizada e contínua, a efetividade dos controles e a potencialidade (probabilidade de ocorrência *versus* impacto) dos riscos, possibilitando a detecção de exposições indesejadas e a implantação de medidas preventivas e corretivas.

A adoção dessas ferramentas tem gerado bons resultados no que se refere à: (i) identificação dos eventos (riscos ou oportunidades) que podem afetar as atividades empresariais; (ii) avaliação dos níveis de exposição; e (iii) definição de planos de melhoria que conduzam a empresa a um ambiente de controle adequado.

No entanto, é necessário evitar que os controles em operação estejam aquém do necessário ou que se configurem dispêndios excessivos para controlar riscos que não representem um potencial de perda relevante. Trata-se, portanto, de um problema de otimização da relação entre o nível de controle desejado e os custos dos controles necessários.

Buscando equacionar esse problema de otimização, o *Committee of Sponsoring Organizations of the Treadway* (COSO) desenvolveu uma metodologia de avaliação baseada na relação custo/benefício associada a cada alternativa de controle – o modelo COSO ERM ou COSO II.

Como abordado no capítulo 2, esse modelo é aplicável a qualquer área de negócio e provê orientações para a investigação da origem dos riscos, permitindo monitorar suas causas e providenciar a mitigação. Esse foi o modelo de escolha para fins da presente pesquisa, por ter se tornado referência para empresas e outras organizações avaliarem e aperfeiçoarem seus sistemas de controle interno, desde a sua criação. Sua estrutura analítica vem sendo incorporada até na formulação de políticas públicas e na elaboração de normas e regulamentos adotados por milhares de organizações em todo o mundo.

A metodologia para hierarquização das regras de monitoramento no âmbito de um projeto de auditoria contínua de uma empresa do setor elétrico brasileiro foi baseada na gestão de riscos e fundamentada no modelo COSO ERM, como apresentado a seguir.

4.1. Base conceitual da metodologia: auditoria baseada em gestão de risco

A gestão de risco, também conhecida pela sigla ERM, é um processo contínuo e conduzido pelas empresas para melhor identificar, entender e responder aos riscos prioritários, como por exemplo: (i) estratégicos; (ii) financeiros; (iii) operacionais; e (iv) de conformidade.

A metodologia baseada em gestão de riscos, objeto deste capítulo, compreende as seguintes etapas:

- identificação de eventos de riscos;
- avaliação de riscos;
- análise da dependência de bases de dados;
- seleção e priorização de processos que serão objeto das atividades de monitoramento e auditoria contínua.

4.1.1. Identificação de eventos de riscos

A identificação dos eventos de riscos que mais poderão afetar os resultados da empresa em foco é o passo inicial para a seleção e priorização dos processos auditáveis considerados críticos para a empresa.

Para a identificação de eventos de riscos, o COSO sugere às empresas o uso de uma combinação de técnicas e ferramentas de apoio. As técnicas de identificação de riscos examinam tanto o passado quanto o futuro. As técnicas voltadas a eventos passados consideram questões como o histórico de falta de pagamento, as mudanças em preços de *commodities* e os incidentes que implicaram em perda de tempo. As técnicas que enfocam eventos futuros consideram questões como mudanças nas características demográficas, novas condições de mercado e ações da concorrência.

Essas técnicas podem apresentar grande variação quanto à sofisticação. No entanto, a maior parte das empresas adota as abordagens mais simples que contemplam a análise de eventos com base em percepções internas dos empregados.

Apresentam-se no Quadro 4.1, a seguir, exemplos de técnicas de identificação de eventos arriscados.

O grau de profundidade, de amplitude e de disciplina na identificação de eventos de riscos pode variar de uma empresa para outra. A administração seleciona as técnicas compatíveis com a sua filosofia de gestão de riscos, buscando assegurar que sejam desenvolvidas as funcionalidades necessárias de identificação de eventos e que as ferramentas de apoio sejam implantadas. De um modo geral, a identificação necessita ser eficazpelo fato de ser a base dos componentes da matriz de riscos e da futura resposta a esses.

Outro ponto de destaque é que, em geral, os eventos de risco não ocorrem de forma isolada. Um evento poderá desencadear outro, e ocorrer concomitantemente. Para identificar os eventos, a administração deve entender o modo pelo qual eles se interrelacionam.

Quadro 4.1 - Exemplos de técnicas de identificação de riscos

Técnica	**Definição**
Inventário de eventos	Trata-se da relação detalhada de eventos em potencial comuns às empresas de um cenário industrial ou ainda para um determinado tipo de processo, ou atividade, comum às empresas daquele cenário. Alguns softwares podem gerar listas de eventos relevantes originárias de uma base geral de potenciais eventos.
Análise interna	Pode ser realizada como parte da rotina do ciclo de planejamento de negócios, tipicamente por meio de reuniões dos responsáveis pela unidade de negócios. A análise interna pode dispor das informações de outras partes interessadas (clientes, fornecedores e outras unidades de negócios) ou da consulta a um especialista no assuntode fora da unidade (ou pessoal interno de auditoria).
Alçadas e limites	Esses gatilhos servem para alertar a administração por meio da comparação dos dados referentes a transações que vem ocorrendo com critérios predefinidos. Uma vez acionado o gatilho, um evento poderá necessitar de nova avaliação ou de uma resposta imediata. Por exemplo, a administração de uma empresa monitora o volume de vendas para receber novos programas de marketing e redireciona seus recursos com base nos resultados. Outra empresa pesquisa as estruturas de preços da concorrência e considera a hipótese de alterar os seus próprios preços se um limite específico for atingido.
Oficinas de trabalho e entrevistas	Essas técnicas identificam eventos com base na experiência e no conhecimento acumulado da administração, do pessoal empregado ou de outras partes interessadas por meio de discussões estruturadas. O facilitador lidera um debate sobre eventos que possam afetar o atingimento dos objetivos da empresa ou de uma de suas unidades. Por exemplo, a realização de uma oficina de trabalho com a particiapção de membros da equipe de contabilidade para identificar eventos capazes de impactar os objetivos de comunicação externa das informações financeiras da organização. Ao combinar o conhecimento e a experiência dos membros da equipe, podem-se identificar importantes eventos que, de outro modo, poderiam passar despercebidos.
Análise de fluxo de processo	Essa técnica congrega as entradas, as tarefas, as responsabilidades e as saídas que se combinam para formar um processo. Considerando-se os fatores internos e externos que afetam as entradas ou as atividades de um determinado processo, a empresa identifica os eventos que podem afetar o cumprimento dos objetivos desse processo. Por exemplo, um laboratório médico mapeia os seus processos de recebimento e análise de amostras de sangue. Ao utilizar mapas de processo, o laboratório considera uma série de fatores que podem afetar as entradas, as tarefas e as responsabilidades, identificando os riscos relacionados com a rotulagem de amostras, as transferências do fluxo dentro do processo e as mudanças de turno do pessoal.
Metodologias de dados sobre eventos de perda	As bases de dados sobre eventos individuais de perdas passadas são uma fonte útil de informações para identificar as tendências e a raiz dos problemas. Após ter identificado uma raiz, a administração poderá decidir que é mais eficaz avaliá-la e tratá-la do que abordar eventos individuais. Por exemplo, uma empresa que opera uma grande frota de automóveis mantém uma base de dados de reclamações de acidentes e, mediante análise, constata que um percentual desproporcional de acidentes, em número e valor monetário, está associado a motoristas de determinadas unidades, área geográfica ou faixas etárias. Essa análise permite que a direção identifique as causas dos eventos e adote as medidas necessárias.

Quadro 4.1 - Exemplos de técnicas de identificação de riscos (cont.)

Técnica	Definição
Indicadores preventivos de eventos	Ao monitorar dados associados aos eventos de riscos, a empresa pode identificar a existência de condições que poderiam originar um evento. Por exemplo, as instituições financeiras, desde há muito, reconhecem a correlação entre os atrasos nos pagamentos de empréstimos e a eventual inadimplência nestes e o efeito positivo de uma intervenção precoce. O monitoramento de padrões de pagamento permite que o potencial de inadimplência seja reduzido por uma ação oportuna.

Fonte: COSO, 2004.

A título de ilustração, a Deloitte apresenta na Figura 4.1 exemplos de riscos de negócio associados aos objetivos: (i) assegurar receita; (ii) otimizar custos operacionais; (iii) eficiência de ativos; e (iv) atendimento das expectativas (Deloitte, 2010).

Figura 4.1 – Eventos de riscos associados a objetivos de negócio, segundo Deloitte (2010)

Fonte: Deloitte, 2010.

A avaliação dos relacionamentos permite determinar em que pontos os esforços da gestão de riscos deverão ser direcionados. Por exemplo, uma mudança na taxa de juros do Banco Central afeta as taxas de câmbio, que é relevante aos ganhos e às perdas nas transaçõesde uma empresa. A decisão de reduzir o investimento em capital postergará um aperfeiçoamento dos sistemas de gestão de

distribuição e ocasionará um tempo de paralisação adicional e uma elevação nos custos operacionais.

4.1.2. Avaliação e priorização de riscos

A avaliação de riscos permite que uma empresa considere até que ponto eles poderiam impactar a realização de seus objetivos. A administração avalia os eventos com base em duas variáveis – probabilidade de ocorrência e impacto financeiro ou sobre a reputação – e, geralmente, utiliza para tal uma combinação de métodos qualitativos e quantitativos. Embora alguns fatores sejam comuns às empresas em geral, os eventos resultantes são singulares em relação a uma determinada organização.

Ao avaliar riscos, a administração leva em consideração eventos previstos e imprevistos. Muitos eventos são rotineiros e recorrentes e já foram abordados nos programas de gestão e orçamentos operacionais, enquanto que outros são imprevistos. A administração avalia os riscos em potencial de eventos imprevistos e, caso ainda não tenha feito essa avaliação, até os previstos que podem causar um impacto significativo na organização.

Risco inerente e residual

A administração leva em conta tanto o risco inerente quanto o residual. Risco inerente é o risco que uma empresa terá de enfrentar caso não tome nenhuma medida para mitigá-lo como, por exemplo, fazer um seguro. Risco residual é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes. Após o desenvolvimento das respostas aos riscos, a administração passará a considerar os riscos residuais.

Estimativa da probabilidade e do impacto

O risco é avaliado levando-se em consideração a perda que poderia ser ocasionada pelo evento de efeitos adversos (impacto) ponderada pela sua probabilidade de ocorrência. A probabilidade representa a possibilidade de que um determinado evento ocorra, enquanto o impacto representa o seu efeito em valor. A administração reconhece que um risco com reduzida probabilidade de ocorrência e baixo potencial de impacto, geralmente, não requer maiores

considerações. Por outro lado, um risco com elevada probabilidade de ocorrência e um potencial de impacto significativo demanda atenção considerável. As circunstâncias situadas entre esses extremos geralmente são difíceis de julgar. É importante que a análise seja racional e cuidadosa.

Técnicas de avaliação

A metodologia de avaliação de riscos de uma organização inclui uma combinação de técnicas qualitativas e quantitativas. Geralmente, a administração emprega técnicas qualitativas de avaliação se os riscos não se prestam a quantificação, ou se não há dados confiáveis em quantidade suficiente para a realização das avaliações quantitativas, ou, ainda, se a relação custo-benefício para obtenção e análise de dados não for viável. Tipicamente, as técnicas quantitativas emprestam maior precisão e são utilizadas em atividades mais complexas e sofisticadas para suplementar as técnicas qualitativas.

As técnicas quantitativas de avaliação geralmente requerem mais esforço e rigor, muitas vezes utilizando modelos matemáticos não triviais. As técnicas quantitativas dependem sobremaneira da qualidade dos dados e das premissas adotadas e são mais relevantes para exposições que apresentem um histórico conhecido, uma frequência de sua variabilidade e que permitam uma previsão confiável.

O Quadro 4.2 exemplifica as principais técnicas de avaliação de riscos.

Segundo COSO (2004), quando há uma escolha híbrida de técnicas de avaliação qualitativas e quantitativas, a administração realiza uma avaliação geral (qualitativa) sobre as medidas de ambas, assim o resultado combinado é expresso em termos qualitativos. O estabelecimento de termos comuns de probabilidade e do grau de impacto para serem adotados por toda a empresa e de termos específicos por categorias comuns de riscos facilita as avaliações de riscos que combinam técnicas qualitativas e quantitativas.

Quadro 4.2 - Exemplos de técnicas de avaliação e priorização de riscos

Técnica	**Definição**
Técnicas qualitativas	Para obter consenso sobre a probabilidade e o impacto de eventos de risco nas técnicas qualitativas de avaliação, poderá ser utilizada a mesma abordagem qualitativa adotada a identificação dos riscos como, por exemplo, identificação de listas de riscos e controles internos, entrevistas, reuniões e oficinas de trabalho. Um processo de auto-avaliação de riscos colhe as opiniões dos participantes a respeito da probabilidade e do impacto de eventos futuros, utilizando escalas descritivas ou numéricas. O exame da relação entre a probabilidade e o impacto dos eventos de risco representa uma importante responsabilidade gerencial. O gerenciamento de riscos corporativos eficaz requer que a avaliação de risco seja efetuada em relação aos riscos inerentes e, também, residuais, conforme descrito anteriormente.
Comparação com referências de mercado (Benchmarking)	É um processo cooperativo entre um grupo de organizações. O benchmarking enfoca eventos ou processos específicos, compara medições e resultados utilizando métricas comuns, bem como identifica oportunidades de melhoria. Dados de eventos, processos e medidas são desenvolvidos para a comparação de desempenho. Algumas companhias utilizam o benchmarking para avaliar a probabilidade e o impacto de eventos em potencial em uma indústria.
Modelos probabilísticos	Os modelos probabilísticos associam a uma gama de eventos e seu respectivo impacto, a probabilidade de ocorrência sob determinadas condições ou segundo premissas preestabelecidas. A probabilidade e o impacto são avaliados com base em dados históricos ou resultados simulados que refletem hipóteses de comportamento futuro. Os exemplos de modelos probabilísticos incluem valor em risco (value-at-risk), fluxo de caixa em risco, receitas em risco e distribuições de prejuízo operacional e de crédito. Os modelos probabilísticos podem ser utilizados com diferentes horizontes de tempo para estimar os seus resultados, como a faixa de prazos dos instrumentos financeiros disponíveis. Os modelos probabilísticos também podem ser usados para avaliar resultados esperados ou médias em relação a impactos imprevistos ou extremos.
Modelos não probabilísticos	Os modelos não probabilísticos empregam critérios subjetivos para estimar o impacto de eventos, sem quantificar uma probabilidade associada. A avaliação do impacto de eventos baseia-se em dados históricos ou simulados a partir de hipóteses sobre o comportamento futuro. Os exemplos de modelos não probabilísticos incluem medições de sensibilidade, testes de estresse e análises de cenários.

Fonte: COSO (2004).

Quando se dispõe de dados quantitativos, os níveis de exposição (alto, médio ou baixo) podem ser mensurados multiplicando-se os impactos pela probabilidade de ocorrência dos eventos de riscos.

A Figura 4.2 ilustra um exercício de análise dos riscos, tendo como foco os eventos de riscos apresentados na Figura 4.1 pela Deloitte (2010).

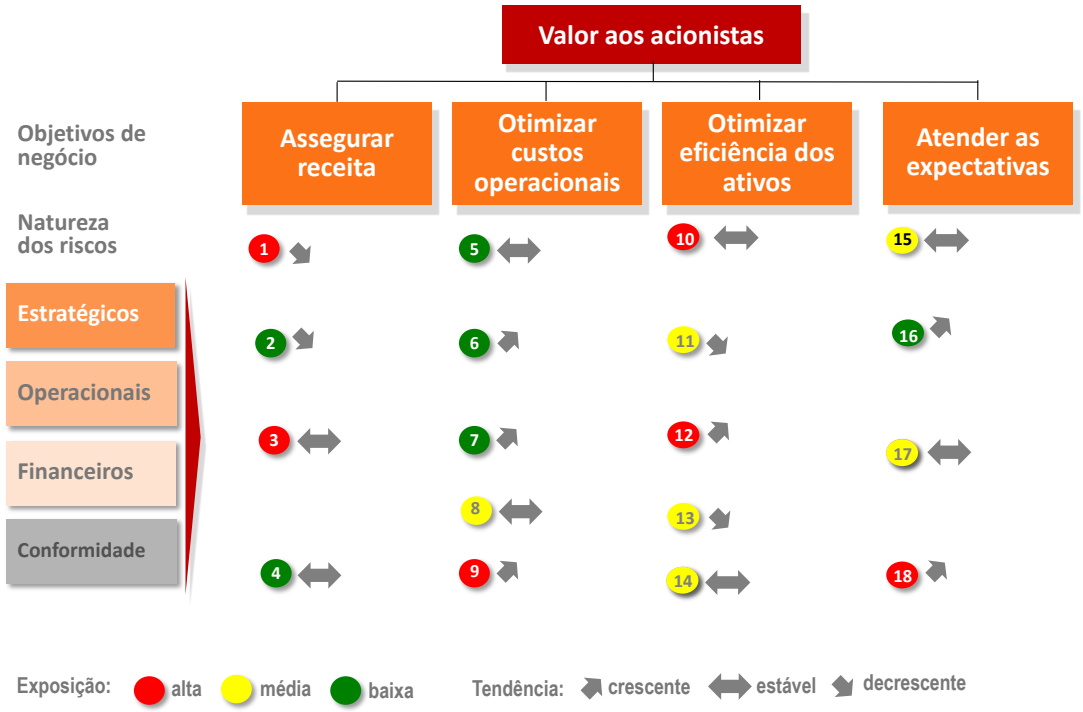

Figura 4.2 – Exemplo de análise de eventos de riscos associados a objetivos de negócio, segundo Deloitte (2010)

Fonte: Deloitte, 2010.

4.1.3. Matriz de risco segundo modelo COSO ERM

Uma vez avaliados os riscos, a priorização pode ser instrumentalizada pela construção de uma matriz, na qual a exposição ao risco definida na etapa anterior é plotada no espaço matricial, segundo as duas variáveis de avaliação: (i) probabilidade de ocorrência; e (ii) impacto. Essas variáveis associam-se aos eventos de riscos (perdas potenciais) inerentes a cada processo.

A tabulação dos riscos em uma matriz permite a clara e ordenada identificação daqueles riscos que poderão impactar mais gravemente os objetivos de negócio de uma empresa. Normalmente, adota-se uma classificação qualitativa para os níveis de probabilidade de ocorrência e de impacto, que poderá variar em função do processo avaliado, do porte da empresa, do segmento de mercado de atuação da empresa, entre outros fatores.

A Figura 4.3 representa um exemplo fornecido pela Deloitte referente a uma matriz de risco construída a partir dos resultados da avaliação mostrada na Figura 4.2.

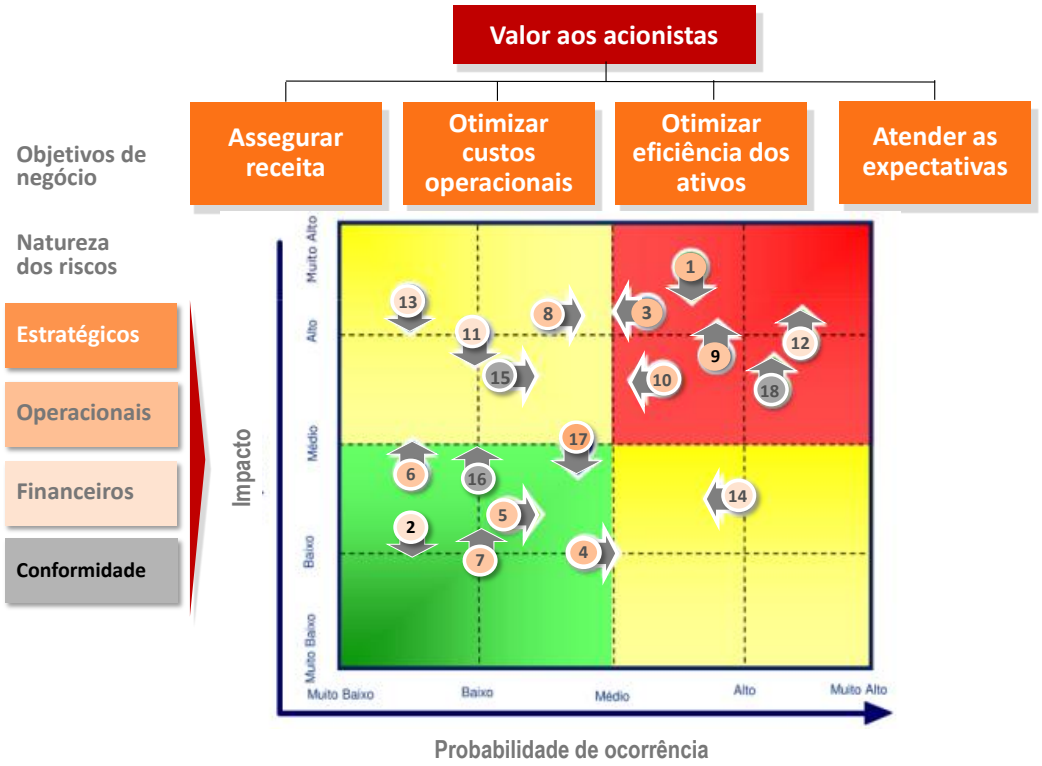

Figura 4.3 – Construção da matriz de riscos associados a objetivos de negócio, segundo o modelo COSO ERM

Fonte: Deloitte, 2010.

4.1.4
Análise da dependência de bases de dados

Um aspecto importante a ser considerado na seleção e priorização de riscos e respectivos processos é a dependência de bases de dados para fins da auditoria contínua e a existência (ou não) de controles internos relacionados aos riscos mais graves.

As estimativas de probabilidade de ocorrência e do grau de impacto de riscos são normalmente conduzidas, utilizando-se dados de eventos passados observáveis. Os dados gerados internamente e embasados na experiência passada da própria empresa podem ser menos subjetivos e propiciar melhores resultados do que os dados de fontes externas.

No entanto, os dados externos também podem ser úteis para aprimorar a análise. Por exemplo, a administração da empresa, ao avaliar o risco de paralisações do fornecimento em razão de falhas de equipamentos, verifica primeiramente a frequência e o impacto de falhas anteriores de seus próprios

equipamentos. Em seguida, complementa esses dados com indicadores de desempenho do ramo de negócio em que atua. Esse procedimento possibilita uma estimativa mais precisa da probabilidade de ocorrência e do impacto de falhas.

4.1.5.
Seleção e priorização de processos auditáveis

A construção da matriz de riscos segundo o modelo COSO ERM permite selecionar e priorizar aqueles eventos de riscos considerados críticos (muito alta ou alta probabilidade de ocorrência *versus* muito alto ou alto impacto). A esses eventos de riscos – situados nos quadrantes vermelho e amarelo da Figura 4.3 – associam-se os respectivos processos e subprocessos da empresa. Esses processos, considerados críticos segundo avaliação de risco, deverão ser objeto da aplicação da ferramenta para hierarquização das regras de monitoramento, na perspectiva do desenvolvimento futuro de uma solução tecnológica de auditoria contínua.

4.2.
Proposta metodológica para estabelecimento e hierarquização das regras de monitoramento

Esta seção apresenta a proposta de uma ferramenta para hierarquização das regras de monitoramento de cada processo crítico selecionado previamente pela empresa em foco, em reuniões estruturadas envolvendo a área de Auditoria Interna e gestores dos processos de nível 1 da empresa.

Assim, para cada processo submetido ao monitoramento e à auditoria contínua deve ser apresentada uma descrição sucinta das principais etapas, para que se identifiquem os pontos de incidência dos eventos de risco de elevado valor de exposição (impacto x probabilidade de ocorrência) no fluxo.

Em seguida, devem ser buscados nos sistemas, ou mediante a realização de oficinas de trabalho, as regras de monitoramento associadas aos eventos de risco, que deverão ser posteriormente hieraquizadas em função de sua importância para o Projeto de P&D e da disponibilidade de informação informatizada.

Os seguintes critérios deverão ser adotados para avaliar a importância de uma determinada regra de monitoramento: (i) cumprimento de regras estabelecidas pela Aneel; (ii) verificação do cumprimento de metas de qualidade no atendimento aos consumidores; (iii) redução de perdas elétricas e financeiras;

(iv) avaliação de controles que tenham o objetivo de mitigar a ocorrência de erros ou fraudes; (v) cumprimento de exigências legais de outros órgãos; e (vi) disponibilidade de informação informatizada.

Para visualização da ferramenta apresentam-se, a seguir, as três matrizes que a integram:

- matriz 1 – descrição das etapas mais expostas a risco em cada processo crítico e identificação de eventos de risco associados (Quadro 4.3);
- matriz 2 – proposição das regras de monitoramento e indicação dos sistemas de informação (Quadro 4.4);
- matriz 3 – hierarquização das regras de monitoramento para fins de auditoria contínua (Quadro 4.5).

Quadro 4.3 – Descrição das etapas mais expostas a risco em cada processo crítico e eventos de risco associados (Matriz 1)

Processo Nível 1: [referência do processo]		
Processo Nível 2: [referência do processo]		
Processo Nível 3	**Etapa**	**Evento de risco associado**
[referência do processo 1]	[descrição da etapa 1]	[eventos de risco 1 a n], se aplicável
	[descrição da etapa 2]	[eventos de risco 1 a n] se aplicável
	[descrição da etapa n]	[eventos de risco 1 a n], se aplicável
[referência do processo 2]	Idem acima	Idem acima
[referência do processo n]	Idem acima	Idem acima

O Quadro 4.4 mostra a Matriz 2 relativa às regras de monitoramento e indicação dos sistemas de informação que fornecerão dados para a plataforma computacional de monitoramento e auditoria contínua. Na coluna à direita, referente à indicação dos sistemas de informação, pode-se incluir para cada regra de monitoramento: (i) sistema(s) de informação; (ii) quem alimenta os dados; e (iii) quem utiliza os dados.

Quadro 4.4 - Proposição das regras de monitoramento e indicação dos sistemas de informação (Matriz 2)

Processo Nível 1: [referência do processo]			
Processo Nível 2: [referência do processo]			
Processo Nível 3	**Evento de risco**	**Regra de monitoramento**	**Sistema de informação**
[referências do processo 1 a n]	[evento de risco 1 identificado na atividade 1]	[regras 1 a n]	[sistemas 1 a n]
	[evento de risco 2 identificado na atividade 1]	[regras 1 a n]	[sistemas 1 a n]
	[evento de risco n identificado na atividade 1]	[regras 1 a n]	[sistemas 1 a n]

Fonte: Elaboração própria, 2013.

O Quadro 4.5, na página seguinte, refere-se à matriz de hieraquização das regras de monitoramento de eventos de riscos para fins de auditoria contínua.

4.3. Aplicação da metodologia de foma participativa

Recomenda-se a aplicação da metodologia em Oficinas de Trabalho organizadas por processo considerado crítico quanto à exposição final ao risco. Essas oficinas deverão contar com a participação de profissionais da empresa em foco envolvidos diretamente nos processos (nível 3) e de representantes das áreas de TI, de Recursos humanos, Logística e Suprimentos, Finanças e da Auditoria Interna. As Oficinas deverão ser conduzidas pela equipe do Projeto de P&D, focalizando-se os seguintes processos (nível 1), a saber: (i) distribuição; (ii) comercialização; e (v) corporativo.

Os objetivos das Oficinas são:

- apresentar uma visão geral do Projeto de P&D e a base conceitual da fase atual do Projeto;
- identificar e registrar as etapas dos processos nível 3, que serão objeto das atividades de auditoria e monitoramento contínuo;
- identificar os eventos de risco associadas às etapas selecionadas dos processos nível 3 e indicar os sistemas de informação que fornecerão dados para a plataforma computacional de monitoramento e auditoria contínua;
- hierarquizar as regras de monitoramento referentes aos processos nível 3;
- promover a troca de informações e conhecimento entre os participantes.

Quadro 4.5 - Hierarquização das regras de monitoramento para fins de auditoria contínua (Matriz 3)

Processo Nível 1: [referência do processo]									
Processo Nível 2: [referência do processo]									
Processo Nível 3	**Evento de risco**	**Regra de monitoramento**	**Importância para o Projeto**						
			ANEEL	**CONSUMIDOR**	**PERDAS**	**ERROS OU FRAUDES**	**OUTRAS EXIGÊNCIAS LEGAIS**	**PONTUAÇÃO**	**HIERARQUIA**
[referência do processo 1]	[evento de risco 1 identificado na atividade 1]	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]
	[evento de risco 2	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]
	[evento de risco n	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]
[referência do processo N]	[evento de risco 1 identificado na atividade 1]	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]
	[evento de risco 2	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]
	[evento de risco n	[regras 1 a n]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[alta - 5, média - 3, baixa -1]	[soma dos pontos]	[posição relativa]

Nota: Critérios para hierarquizar regras de monitoramento segundo importância para o projeto de auditoria contínua: (i) cumprimento de regras estabelecidas pela Aneel (ANEEL); (ii) verificação do cumprimento de metas de qualidade no atendimento aos consumidores (CONSUMIDOR); (iii) redução de perdas elétricas e financeiras (PERDAS); (iv) avaliação de controles que tenham o objetivo de mitigar a ocorrência de erros ou fraudes (ERROS ou FRAUDES); (V) cumprimento de exigências legais de outros órgãos (OUTRAS EXIGÊNCIAS LEGAIS).

Durante as Oficinas serão desenvolvidas atividades em grupos direcionadas para geração dos seguintes resultados:

- entendimento sobre o Projeto de P&D e a base conceitual da fase atual do Projeto;
- processos (nível 3) que serão objeto das atividades de auditoria e monitoramento contínuo;
- etapas dos processos nível 3 de maior exposição a riscos e os eventos de risco associados (Matriz 1);
- regras de monitoramento referentes aos eventos de risco e indicação dos sistemas de informação (Matriz 2);
- regras de monitoramento hierarquizadas (Matriz 3);
- troca de informações e conhecimento entre os participantes.

A duração proposta para as Oficinas é de um dia e meio, conforme programação-padrão apresentada abaixo no Quadro 4.6.

Quadro 4.6 – Programação-padrão para as Oficinas de Trabalho

1º dia	
Horário	**Atividade**
09:00 – 09:30	Abertura dos trabalhos e apresentação geral do Projeto P&D, situando a etapa #3 – plenária
09:30 – 10:00	Apresentação das bases conceituais e da metodologia geral da Oficina (PUC-Rio) – plenária
10:00 – 12:00	**Atividade 1 -** Descrição das etapas dos processos nível 3 mais expostas a riscos e identificação de eventos de risco associados (Matriz 1) – atividade em grupos (por processo)
12:00 – 14:00	**Almoço**
14:00 – 16:50	**Atividade 2** – Proposição de regras de monitoramento referentes aos eventos de risco identificados na Atividade 1 e indicação dos sistemas de informação (Matriz 2) – atividade em grupos (por processo)
16:50 – 17:00	**Encerramento das atividades do 1º dia da Oficina de Trabalho (plenária)**
2º dia	
Horário	**Atividade**
09:00 – 10:30	**Apresentações dos grupos - Atividades 1 e 2 (plenária)**
10:30 – 11:30	**Atividade 3 –** Hierarquização das regras de monitoramento para fins de auditoria e monitoramento contínuo (Matriz 3) – atividade em grupos (por processo)
11:30 – 12:00	**Encerramento da Oficina de Trabalho e próximos passos (plenária)**

Cabe ressaltar que a eficácia do planejamento de eventos dessa natureza está diretamente ligada a um desenho metodológico definido a partir de uma delimitação precisa das questões a serem respondidas, da proposta de

sistematização do processo e da escolha criteriosa dos participantes e especialistas envolvidos.

4.4. Considerações sobre a aplicabilidade da metodologia em uma empresa do setor elétrico brasileiro

Neste capítulo, propôs-se uma ferramenta para hierarquização das regras de monitoramento de cada processo crítico selecionado para fins de desenvolvimento de uma solução tecnológica para monitoramento e auditoria contínua a ser adaptada pela empresa em foco. Inclui-se ao final uma proposta para aplicação da ferramenta mediante a realização de Oficinas de Trabalho na empresa, com a participação de profissionais envolvidos diretamente nos processos (nível 3) e de representantes das áreas de TI, de Recursos Humanos, de Finanças, de Logística e Materiais e da Auditoria Interna. Recomenda-se a realização de duas Oficinas no segundo semestre de 2013, como parte fundamental do desenvolvimento da Etapa #3 do Projeto de P&D.

Acredita-se que o mapeamento dos processos – visando primordialmente hierarquizar e priorizar as regras de monitoramento e realizar um diagnóstico inicial sobre os sistemas de informação que fornecerão dados para as atividades de monitoramento e auditoria contínua – possa contribuir de forma significativa para o sucesso do desenvolvimento da plataforma computacional pela empresa europeia, como previsto no Termo de Referência do Projeto.

A associação de processos críticos a respostas a riscos e regras de monitoramento contínuo é ilustrada no exemplo a seguir fornecido por COSO (2004): uma empresa estabelece como objetivo alcançar ou exceder as metas de vendas, identificando como risco a falta de conhecimentos dos fatores externos, como por exemplo, as necessidades atuais ou potenciais dos clientes. Para reduzir a probabilidade da ocorrência e o impacto do risco, a administração recorre aos históricos de compras dos clientes existentes e empreende novas iniciativas de pesquisa de mercado.

As respostas a riscos neste exemplo servem de referência para estabelecer regras de monitoramento nos respectivos subprocessos (ou atividades) e, também, acompanhar o progresso e o desenvolvimento do histórico de compras de clientes

em relação às programações estabelecidas e à adoção de medidas para assegurar a precisão dos dados relatados.

Ao selecionar regras de monitoramento contínuo, a Auditoria Interna considera a forma como essas atividades se relacionam entre si. Em alguns casos, uma única regra pode abordar diversas respostas a riscos. Em outros, diversas regras de monitoramento são necessários para apenas uma resposta a risco. E, ainda, em outras situações, a área de Auditoria Interna poderá constatar que as regras de monitoramento existentes são suficientes para assegurar a execução eficaz das respostas a riscos.

Na prática, o que vem sendo adotado é uma combinação de regras de monitoramento para prover respostas relacionadas a riscos. Por exemplo, quando a administração de uma empresa estabelece limites para transações (para administrar os riscos relacionados com um dado portfólio de investimentos), gera regras de monitoramento específicas para assegurar que os limites das transações não sejam ultrapassados. As regras de monitoramento incluem os limites preventivos, que evitam a concretização de determinadas transações, e os de detecção, que identificam oportunamente outras transações discrepantes.

A implantação do monitoramento e auditoria contínua com regras automatizadas visa assegurar que todas as informações sejam colhidas corretamente e que os procedimentos de rotina permitam que os indivíduos responsáveis autorizem ou aprovem as decisões de forma correta. Além disso, citam-se outros importantes fatores, dentre os quais o atendimento à Lei Sarbanes-Oxley e a necessidade da divulgação financeira confiável para todas as partes interessadas.

De fato, a auditoria contínua ou em tempo real emerge como recurso ferramental avançado para o acompanhamento e monitoração em tempo real (ou quase real) dos processos e negócios empresariais, mediante a adoção de mecanismos de controle incorporados nos sistemas de informação empresariais ou mediante a utilização de *software* apropriado, como a solução tecnológica que será desenvolvida para a empresa em foco no âmbito do referido Projeto de P&D.