



Síntese e Resultados da 9ª mesa de debates
Sox Update e Avaliação do Ambiente de
Controle (COSO) - Outubro de 2006

10ª mesa de debates
Governança e Fraudes em TI - Março de 2007

AUDIT COMMITTEE INSTITUTE DA KPMG NO BRASIL



Síntese da 9ª mesa de debates Sox Update e Avaliação do Ambiente de Controle (COSO)

A Nona Mesa de Debates do ACI contou com a ilustre participação do Sr. Leonardo Moretzsohn da Cia. Vale do Rio Doce (CVRD), que apresentou o desenvolvimento do projeto Sarbanes–Oxley na companhia. O Sr. Leonardo Moretzsohn está na CVRD desde 1983 e atualmente é diretor de controles internos. Atuou em diferentes áreas dentro da organização, como por exemplo, desenvolvimento de negócios, comercial e financeiro. O Sr. Sidney Ito, sócio da área de Risk Advisory Services da KPMG no Brasil, também atuou como palestrante e apresentou o resultado de um estudo realizado a partir da análise dos 20Fs das empresas brasileiras registradas na SEC.

O material referente à palestra do Sr. Sidney Ito, com uma atualização sobre o cenário atual das empresas em processo de adequação e o uso do frame work COSO, foi entregue no próprio dia.

Painelista

Leonardo Moretzsohn,

Diretor de Controles Internos

Cia. Vale do Rio Doce

A apresentação do Sr. Leonardo teve como principal objetivo compartilhar a experiência vivida no processo de implementação dos requerimentos da *Lei Sarbanes-Oxley (SOX)* na CVRD. O texto a seguir foi elaborado com base nesta apresentação.

Após o início do projeto, em julho de 2004, a empresa passou por uma série de adequações e de adaptações, que visavam um processo tranquilo de certificação.

Esse esforço também objetivou mostrar o trabalho realizado aos acionistas, como uma forma de evolução no processo de informação e transparência e na manutenção dos elevados níveis de Governança Corporativa.

Importância da Certificação Sarbox para a Vale

- ✓ Aproximadamente 55% do *free float* são negociados sob a forma de ADRs (*American Depositary Receipts*) na Bolsa de Valores de Nova York (NYSE).
- ✓ Manutenção do registro na SEC (*Security Exchange Commission*) e NYSE.
- ✓ Mercado americano como consumidor de diversos produtos da CVRD: minério de ferro, pelotas, caulim, ferro ligas e outros.



Entendendo os requerimentos da SOX

Na CVRD acredita-se que governança corporativa é algo muito importante, em razão de ter uma grande parcela do seu capital disponibilizado no mercado. Por isto, a transparência, a maneira como atua com os empregados, com a sociedade e com os acionistas, faz parte do dia-a-dia da empresa. A Lei Sarbanes-Oxley (SOX) passou a integrar esse escopo e a ser considerada de suma importância. Leonardo entende que a lei visa primordialmente responsabilizar a administração das empresas, principalmente o CEO e o CFO, sobre as demonstrações contábeis e a eficácia dos controles internos, e que proporciona maior confiabilidade e transparência por meio de um ambiente de controle eficaz e pela maior cobrança de responsabilidade por parte dos auditores independentes, garantindo assim maior segurança para os acionistas.

Com 55% das ações negociadas no mercado norte americano, o que gera uma grande exposição naquele mercado, que além de ser um grande mercado acionário é também um grande mercado para os seus produtos, o projeto SOX não poderia ter sido encarado de outra forma, que não a preocupação da empresa em se criar uma estrutura que estivesse dedicada a adequar a CVRD a atender esses requisitos. Uma falha no processo de certificação seria inadmissível. Uma empresa com tal ambição de crescimento e de se tornar

global, tem que atender a todos os requisitos legais, sejam eles quais forem. No primeiro momento a sensação é de estar diante de uma caixa-preta, citou Leonardo, afinal era uma lei feita em um outro país, com um outro ambiente legal e regulatório, e com um ônus de desvendar as exigências dessa lei. A CVRD decidiu então criar um departamento de forma a entender e destrinchar esse ambiente regulatório e planejar adequadamente o desafio que viria a seguir. Por intermédio de consultorias, seminários e conversas com parceiros norte-americanos procuraram entender qual era o espírito da lei, o que a lei efetivamente buscava conquistar e onde precisariam adequar os sistemas e processos para atender essa certificação. Neste momento, o COSO foi definido como o modelo de estrutura de controles internos a ser perseguido e implementado.

A SOX é uma lei com mais de 900 seções, mas nem todas aplicáveis a CVRD. Algumas adequações foram feitas para atendimento de seções específicas, como por exemplo as seções 201 e 203, para as quais foi necessário adotar e criar uma norma que regulasse toda a contratação e prestação de serviços das empresas de auditoria para a CVRD. Abordou-se então quais serviços que devem ser aprovados, quais são pré-aprovados e um orçamento anteriormente aprovado pelo conselho fiscal (a opção da empresa, num primeiro momento, foi por “turbinar” o conselho fiscal. Todas as transações atuais com os auditores independentes estão reguladas, através de uma norma, e os

serviços devem necessariamente ser avaliados antes da contratação. Há um orçamento pré-aprovado e também faz parte das atividades do conselho fiscal, avaliar e fiscalizar a contratação de serviços e a obediência a essa norma.

Além disto, o conselho conta com um especialista em *financial reporting* e *USGAAP*, e foi criada uma ouvidoria para cuidar do canal de denúncias e disseminar o comportamento ético esperado pela empresa. Esta ouvidoria é a responsável pela apuração de eventuais denúncias de caráter contábil e também de garantir o sigilo e o anonimato durante todo o processo de apuração. Também foi criado um comitê de divulgação de fatos relevantes em tempo real, onde todo e qualquer fato importante da empresa, seja ele demonstração financeira, ou qualquer atividade que possa impactar o valor da empresa, é imediatamente divulgado.

A criação do departamento de controles internos, subordinado ao CFO, a quem cabe a responsabilidade de fazer a certificação dos controles internos de acordo com a seção 404, tem como objetivos adequar os processos e disseminar a cultura de controles internos. Pretende-se avaliar o uso do *Control Self Assessment*, no qual cada área dentro da empresa, independentemente de se ter um controle corporativo centralizado, terá o objetivo de autocertificar e estar absolutamente em *Compliance* quanto à eficiência e a eficácia dos controles internos.

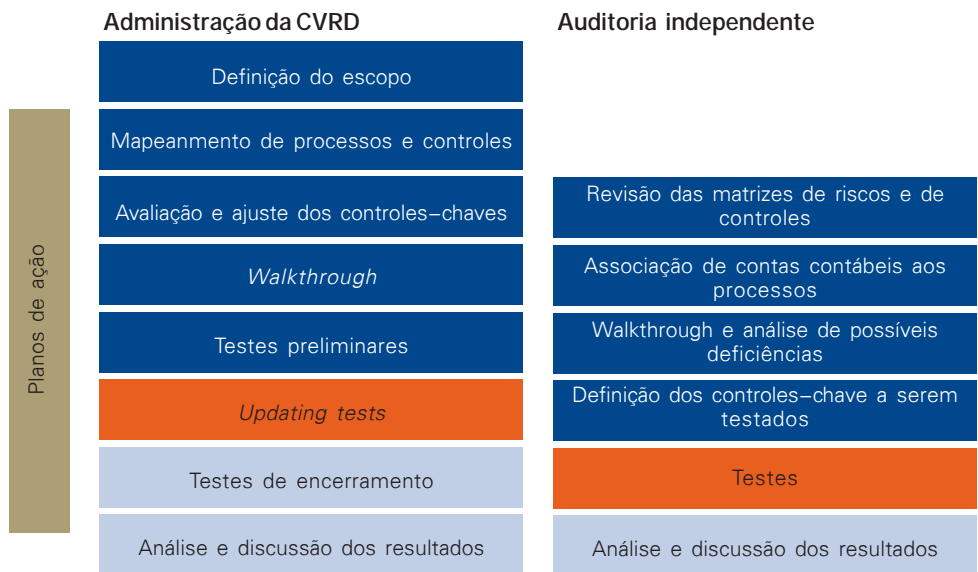
Estratégia da CVRD para adequação à Lei Sarbanes-Oxley

- ✓ Verificou as seções da lei aplicáveis à Companhia, analisou os possíveis impactos e efetuou os ajustes necessários.
- ✓ Criou o Departamento de Controles Internos, subordinado ao CFO, para gerenciar o programa de adequação à lei, em especial à seção 404, que trata de controles internos.
- ✓ Buscou conhecimento adicional sobre a Lei e sua implementação nas empresas americanas, através de participação em seminários nacionais e internacionais, workshops e apoio de empresa de consultoria.
- ✓ Definiu o COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) como modelo de estrutura de controles internos, por ser o mais difundido entre as empresas americanas.

Como um dos objetivos era disseminar a cultura de controles internos, fazendo com que cada atividade, cada subsidiária, tivesse a condição de entender o processo e se responsabilizar por sua própria certificação, mais de 300 profissionais foram treinados por meio de *e-learning* na metodologia COSO, em processos de mapeamento e na avaliação de risco, de forma que cada área, seja ela uma área de mineração, uma área comercial, financeira ou contábil tivessem definidos os responsáveis pelo mapeamento, sendo estes os atuais responsáveis pela gestão da eficácia dos seus controles.

Como forma de garantir que não haveria qualquer problema na certificação, mesmo com o adiamento do prazo inicial de 2005 para 2006, a CVRD decidiu manter a estratégia de atuação inicialmente prevista. Em 2005, foram feitos testes em todos os processos da empresa, mesmo não sendo necessária a certificação naquele ano.

Passos adotados para obter a certificação:



O primeiro passo foi a definição do escopo do que seria certificável em função do conceito de materialidade, identificando as operações da empresa que impactam as demonstrações financeiras, e quais atividades da empresa causam risco às operações como um todo.

Com a matriz no Brasil, sendo a CVRD uma empresa operacional e holding, a certificação recai sobre as 16 empresas, situadas no Brasil e no exterior. Isto significa que não apenas a matriz deve ser considerada, mas também deve-se expandir esse processo de certificação por um universo bem mais amplo. Isto significa um trabalho extra, porque além de trabalhar culturalmente no Brasil, tem que promover este processo em países com culturas diferentes e que tem outras perspectivas de controles internos, como por exemplo, as operações na Noruega, na França, entre outras.

Com mais experiência no assunto, foi possível ajustar o escopo para um universo de 9 empresas, aquelas que efetivamente tem um maior volume de risco financeiro associado.

Dois critérios foram considerados nesta avaliação:

- Qualitativo: os riscos inerentes a cada negócio como alumínio, minério de ferro e manganês e as empresas associadas à estes negócios que imporiam riscos as nossas demonstrações financeiras.
- Quantitativo: com base nas demonstrações contábeis, foram identificadas as contas significativas e os processos e sub-processos relacionados que deveriam ser mapeados.

Com base neste trabalho, foram identificados 15 processos, como tesouraria, contabilidade, vendas, ativo imobilizado e, dentro destes processos, 335 sub-processos, distribuídos em 9 empresas, com um total de 1400 controles-chave. Todos estes controles foram mapeados e são constantemente monitorados, pois são aqueles que se falharem podem não impedir que erros sejam apresentados nas demonstrações financeiras. Foi escolhida um *software* para documentar o processo e a diretoria da empresa estipulou 5 níveis hierárquicos de certificação, de forma a envolver e conscientizar todos os

níveis hierárquicos neste processo de certificação. Isto exige que todos os processos estejam em ordem, com eficácia avaliada, adequadamente descritos, conforme as normas e políticas da empresa, assegurando o conforto necessário ao CFO e ao CEO para assinar a certificação exigida.

Cada diretor de cada departamento de cada operação da CVRD atestou que o ambiente de controle sob sua responsabilidade funciona adequadamente e de uma forma eficaz. Essa foi uma das etapas importantes, que estabeleceu comprometimento de todos os níveis da empresa.

Todo este trabalho inicial vem sendo revisado pelo auditor e a intenção da administração da empresa é uma certificação sem arranhar a imagem, sem nenhum *Material Weakness*. Esta meta foi colocada pela alta administração da empresa, e encarada como uma importante missão pelos gestores.

Durante o mapeamento dos 1400 controles-chaves, foram identificadas as diferenças na constituição destes controles, que mesmo sendo todos eficazes, não eram uniformes. A unificação e a padronização gerou mais eficiência, e isto foi percebido como o primeiro benefício do processo de adequação à *SOX*.

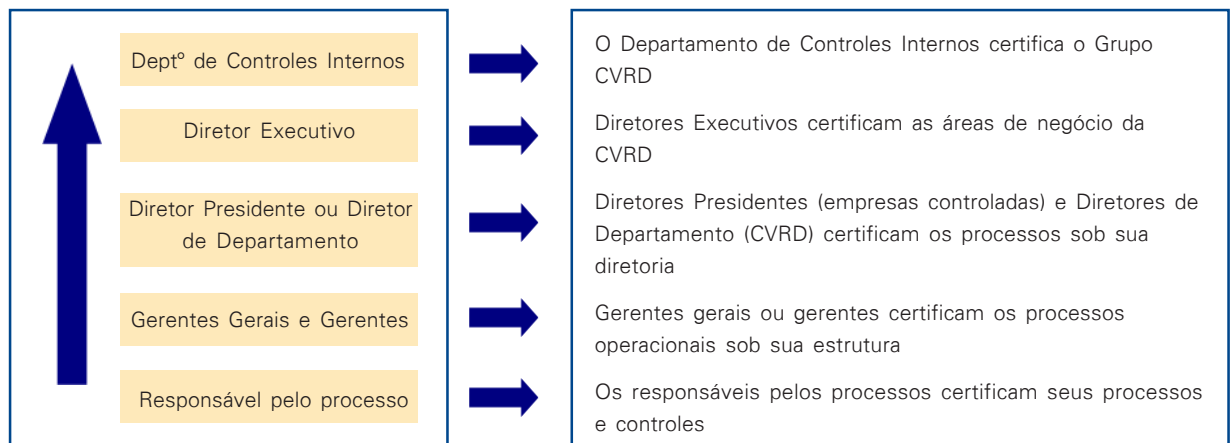
Programa de adequação à Seção 404 da Lei Sarbanes-Oxley

- ✓ Avaliação e definição da abrangência da aplicação da Lei no Grupo CVRD.
- ✓ Mapeamento de processos e avaliação de controles efetuados de forma descentralizada pelas áreas de negócio e empresas controladas, sob a coordenação do departamento de Controles Internos.
- ✓ Treinamento de aproximadamente 300 profissionais na metodologia de mapeamento de processos e de avaliação de riscos (cursos presenciais e *e-learning*).
- ✓ Aquisição e implementação da ferramenta *Risk Navigator* para arquivar a documentação dos processos e controles internos e o resultado da avaliação pela administração, além de servir como instrumento de certificação (*Sign off*).
- ✓ Execução de testes ainda durante o ano de 2005 para verificação da eficácia dos controles internos e da implementação de planos de ação corretivos.

Alguns fatores foram primordiais para o sucesso do projeto. O primeiro foi o patrocínio da alta administração, que incentivou, por meio de exemplo, em um processo top-down, o cumprimento do projeto de forma plena. O fato também de ter contado com uma área centralizada, que coordenou todo o projeto, também foi de suma importância.

A decisão de tocar o projeto de forma descentralizada foi uma decisão que provou-se acertada, porque capacitou as pessoas e disseminou a cultura de riscos e controles na empresa, por meio de uma comunicação permanente. Em todas as publicações da empresa, em todos os encontros, SOX era mencionada. Por último, Leonardo ressaltou a importância de um adequado processo de acompanhamento dos plano de ação para remediação de eventuais falhas constatadas no ambiente de controle e/ou nos controles internos dos processos operacionais. Até mesmo pelo volume e pela abrangência, além dos aspectos de TI e da descentralização, ter um adequado processo de *follow-up* é vital em um projeto desta natureza.

Hierarquia de Certificação adotada na CVRD



Benefícios alcançados

- ✓ Documentação, padronização e otimização de processos, sistemas e controles.
- ✓ Facilitador para o treinamento de novos empregados.
- ✓ Aprimoramento do ambiente de controle e, conseqüentemente, redução dos riscos de fraudes.
- ✓ Acelerador para implantação/substituição de sistemas e controles.
- ✓ Redução do prazo médio de faturamento de minério de ferro e de envio dos documentos de embarque aos clientes.
- ✓ Saneamento de Bancos de Dados.

Resultado da Pesquisa

9ª mesa de debates

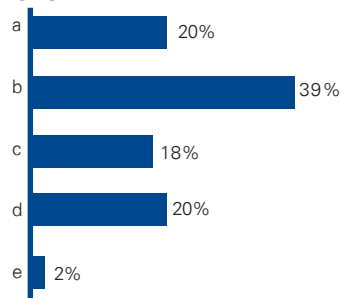
Sox Update e Avaliação do Ambiente de Controle (COSO)

Realizamos uma pesquisa interativa durante a 9ª Mesa de Debates do *Audit Committee Institute - ACI* na qual os participantes puderam se expressar a respeito do tema abordado na ocasião.

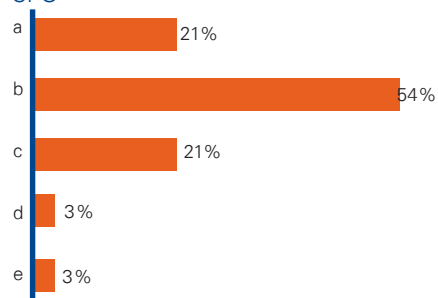
A seguir, transcrevemos os resultados desta pesquisa.

1. Qual o nível de entendimento sobre a Lei SOX e seus impactos que V.Sa. atribui aos responsáveis pelo projeto na sua empresa?
- a) Total conhecimento
 - b) Bom conhecimento
 - c) Regular
 - d) Insuficiente
 - e) Praticamente nulo

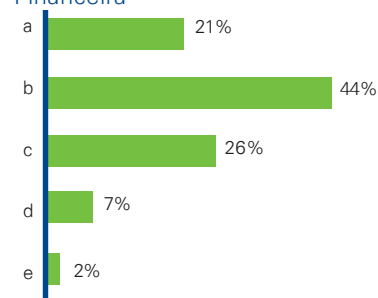
CEO



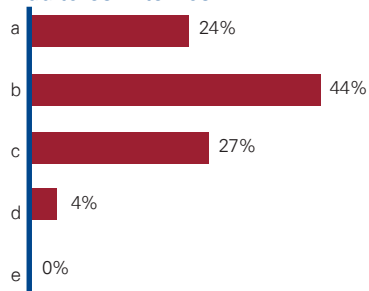
CFO



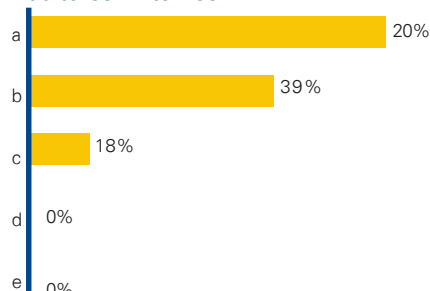
Profissionais da Contabilidade/ Financeira



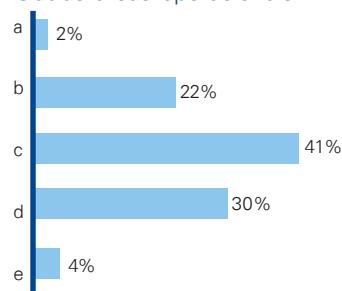
Audidores Internos



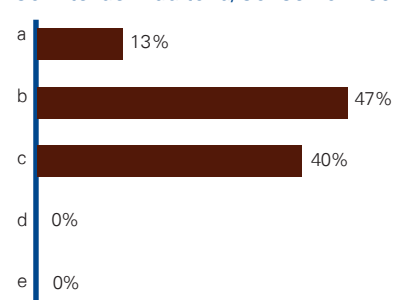
Audidores Externos



Outras áreas operacionais



Comitê de Auditoria/Conselho Fiscal



Em relação ao nível de entendimento do CEO, os conselheiros entendem que a maioria possui conhecimento total ou bom. Porém, deve se destacar que, após quatro anos da promulgação da Lei, ainda, na opinião dos conselheiros, muitos CEOs tem conhecimento apenas regular (18%) ou em uma situação ainda pior, julgam que esse conhecimento é insuficiente ou nulo (22%).

Quanto ao CFO, a percepção é de que o conhecimento é pleno, sendo que 75% o classificou como sendo total ou bom.

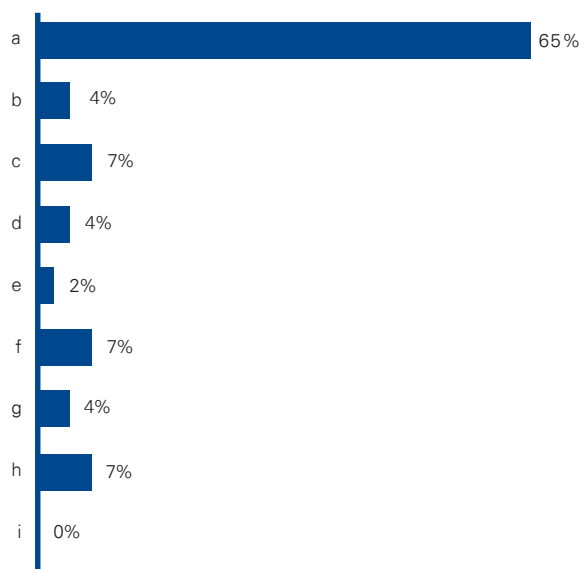
Os conselheiros avaliaram de forma similar os profissionais da contabilidade/ área financeira e os auditores internos, na faixa de 70% de aprovação e com baixo índice de reprovação.

Os auditores externos tiveram a melhor avaliação. Segundo os conselheiros, 54% dos auditores possuem conhecimento total e 37% bom conhecimento.

Em relação às outras áreas operacionais, a avaliação apontou que 30% tem conhecimento insuficiente e apenas 24% tem bom conhecimento. Quanto aos próprios membros de comitê de auditoria e conselho fiscal, 60% considera como conhecimento bom ou superior e 40% entendem ser apenas regular.

2. Para quais dos itens abaixo há o maior risco de serem reportadas é esperado o maior volume de fraquezas materiais nos controles internos?

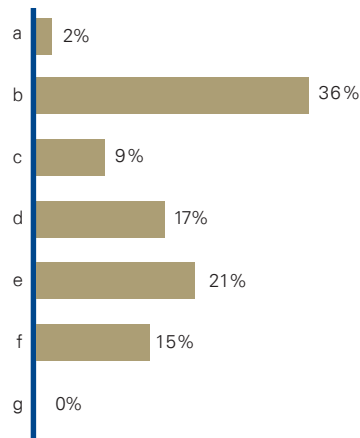
- a) Tecnologia da Informação
- b) Reconhecimento de receita
- c) Gerenciamento do Imobilizado
- d) Compras e contas a pagar
- e) Impostos
- f) Recursos Humanos
- g) Tesouraria
- h) Encerramento e apresentação das demonstrações financeiras
- i) Outros



Para 65%, há uma percepção de que a tecnologia da informação é a que poderá gerar um maior volume de fraquezas materiais. Os demais itens estiveram restritos a uma faixa de 2% a 7%. A título de comparação, pesquisa similar realizada em 2005 teve como resultado uma votação de 57% para TI, o que indica que esta preocupação não é recente e se manteve no mesmo patamar.

3. Qual é o percentual dos controles internos manuais de sua empresa em comparação com os controles automatizados?

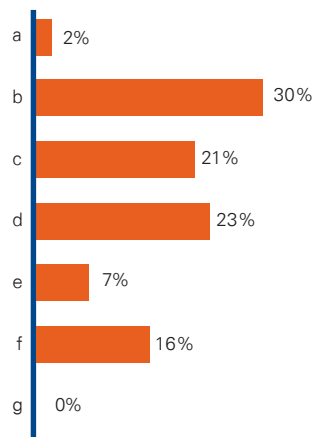
- a) 100% manual
- b) 80% manual vs. 20% automatizado
- c) 60% manual vs. 40% automatizado
- d) 50% manual vs. 50% automatizado
- e) 40% manual vs. 60% automatizado
- f) 20% manual vs. 80% automatizado
- g) 100% automatizado



Em relação ao equilíbrio entre controles manuais e automatizados atualmente existentes, a maioria dos conselheiros (47%) indicou que o volume de controles internos manuais estão em maior quantidade do que os controles automatizados, sendo que 36% afirmaram que o volume de controles automatizados é de apenas 20%.

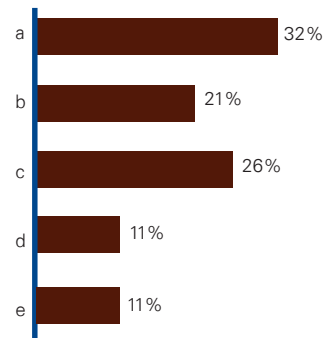
4. Qual é o percentual dos controles internos detectivos de sua empresa em comparação com os controles preventivos?

- a) 100% detectivo
- b) 80% detectivo vs. 20% preventivo
- c) 60% detectivo vs. 40% preventivo
- d) 50% detectivo vs. 50% preventivo
- e) 40% detectivo vs. 60% preventivo
- f) 20% detectivo vs. 80% preventivo
- g) 100% preventivo

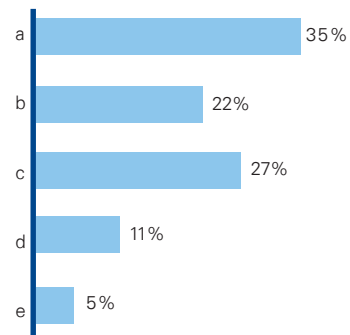


Um quadro bastante similar ao anterior se apresenta para o balanço entre controles internos detectivos ou preventivos. Naturalmente, os controles automatizados tendem a ser preventivos e por esta razão há um volume significativo de controles detectivos (53%) e manuais (47%).

5. Nesse momento, quem é o responsável na sua empresa pela supervisão do projeto de adequação aos requerimentos da SOX 404?
- a) CFO (*Chief Financial Officer*)
 - b) Controller
 - c) Líder da Auditoria Interna
 - d) Gerente de Projeto (especialmente designado para esta função)
 - e) Outros

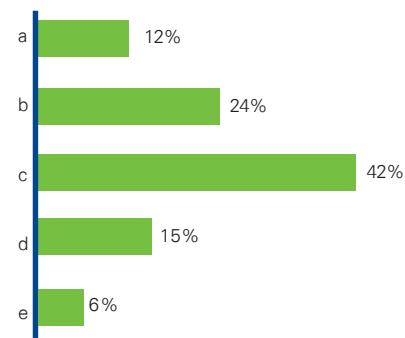


6. Após a primeira certificação, quem será o responsável na sua empresa pela supervisão do SOX 404?
- a) CFO (*Chief Financial Officer*)
 - b) Controller
 - c) Líder da Auditoria Interna
 - d) Gerente de Projeto (especialmente designado para esta função)
 - e) Outros

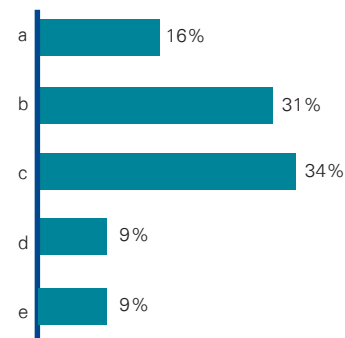


A responsabilidade pela supervisão do Projeto SOX 404 nas empresas está bem dividida entre CFO (32%), Líder da Auditoria Interna (26%) e Controller (21%). Este quadro deve se manter após a primeira certificação.

7. Nesse momento, quem é o responsável na sua empresa pelo gerenciamento do projeto (dia-a-dia) de adequação ao SOX 404?
- a) CFO (*Chief Financial Officer*)
 - b) Controller
 - c) Líder da Auditoria Interna
 - d) Gerente de Projeto (especialmente designado para esta função)
 - e) Outros



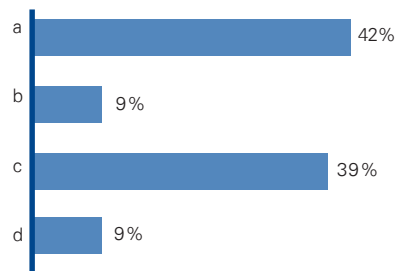
8. Após a primeira certificação, quem será o responsável na sua empresa pelo gerenciamento do projeto do SOX 404?
- a) CFO (*Chief Financial Officer*)
 - b) Controller
 - c) Líder da Auditoria Interna
 - d) Gerente de Projeto (especialmente designado para esta função)
 - e) Outros



Quanto ao gerenciamento do projeto no seu dia-a-dia, em 2006 esta atividade estava a cargo principalmente do líder de Auditoria Interna (42%). Os conselheiros apontaram uma tendência de que este gerenciamento passe a ser de responsabilidade do controller (31%) em muitas empresas, embora o percentual de empresas na qual o líder de auditoria interna será o responsável ainda é a mais relevante (34%).

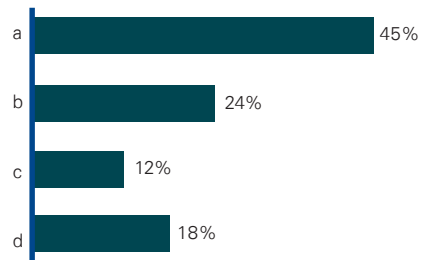
9. A Auditoria Interna da empresa em que atua está envolvida com a elaboração da documentação ou aplicação dos testes exigidos para o cumprimento da SOX 404?

- a) Sim; apenas com recursos próprios
- b) Sim; por meio de terceirização da atividade
- c) Sim; com recursos próprios e terceirização parcial
- d) Não



10. Quem será o principal responsável pela aplicação dos testes necessários para o cumprimento das exigências da SOX 404?

- a) Auditoria Interna
- b) Consultoria contratada
- c) Auto-avaliação
- d) Equipe mista

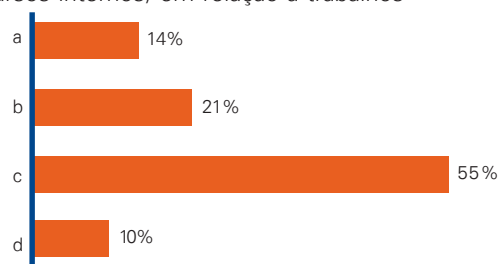


As empresas adotaram como modelo no processo de documentação e testes da SOX 404 a utilização de recursos próprios (42%) ou a terceirização parcial (39%).

Para o exercício seguinte à primeira certificação os testes devem ficar a cargo da auditoria interna (45%) ou de uma consultoria contratada (24%) para estes fins. O recursos de auto-avaliação (12%) ainda tem pouca presença no mercado brasileiro, embora tenha sido uma opção avaliada cuidadosamente em diversos mercados.

11. Qual a representatividade do volume de horas internas (utilização de recursos internos) em relação à trabalhos executados por terceiros para a SOX 404?

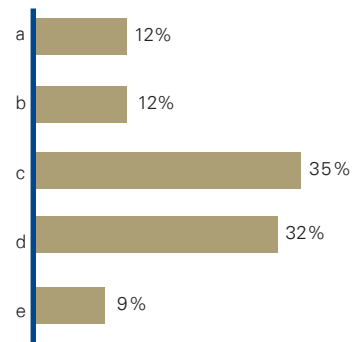
- a) 0% a 25%
- b) 26% a 50%
- c) 51% a 75%
- d) 76% a 100%



A proporção de 51% a 75% de horas de recursos internos em relação aos consultores externos foi a que teve maior citação (55%) pelos conselheiros.

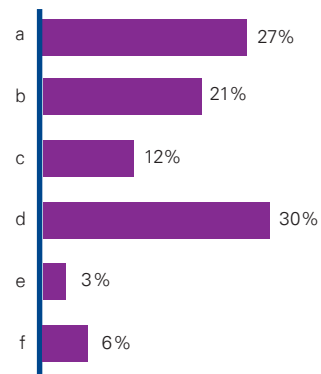
12. No seu entendimento, os custos relativos ao cumprimento da Lei Sarbanes–Oxley 404 nos anos seguintes à primeira certificação irão:

- a) Aumentar
- b) Diminuir mais que 50%
- c) Diminuir entre 50% e 30%
- d) Diminuir entre 30% e 10%
- e) Manter–se no mesmo patamar



13. Em sua opinião, em qual atividade haverá a maior redução desses custos?

- a) Documentação
- b) Planejamento
- c) Aumentando ou reduzindo o número de controles
- d) Honorários de auditores externos
- e) Aplicação de testes
- f) Auto–avaliações
- g) Outros motivos

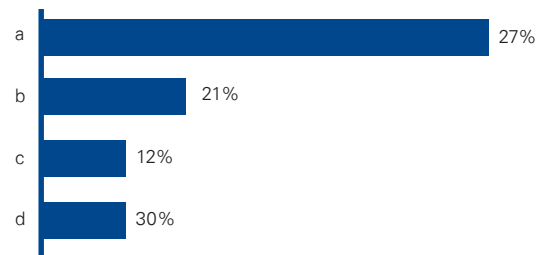


No entendimento dos conselheiros, o custo com a SOX 404 deve diminuir significativamente nos anos seguintes à certificação, sendo que apenas 21% acredita que serão iguais ou no mesmo patamar. Uma redução entre 10% e 50% é esperada por cerca de 67% do público participante de nossa votação.

A maior expectativa é que estas reduções ocorram nos honorários dos auditores externos (40%), etapa de documentação dos processos (27%) e de planejamento (21%).

14. Considerando todos os esforços direcionados para o cumprimento da SOX 404, por favor, relacione uma lista dos três principais benefícios que sua empresa espera obter como resultado desses esforços?

- a) Melhores controles (controles mais eficazes, maior conscientização, documentação, etc.);
- b) Melhores processos (documentação mais adequada, padronizada e enxuta, etc.);
- c) Maior eficácia operacional; ou
- d) Maior conhecimento sobre nossa empresa/compartilhamento das melhores práticas.



Considerando todos os esforços direcionados para atender a SOX 404, o benefício citado pela grande maioria dos votantes (59%) relaciona–se ao aperfeiçoamento dos controles internos, que tornaram–se mais eficazes, melhor documentados e com uma maior conscientização dos gestores sobre a sua importância.

10ª mesa de debates

Gerenciamento dos Riscos de Fraude por meio da Tecnologia da Informação

Introdução

Os casos de fraudes executadas por meio de recursos de Tecnologia da Informação têm se tornado cada vez mais comum nas empresas e por isso faz parte da agenda dos executivos implementar um sistema composto por mecanismos e indicadores de prevenção e detecção de incidentes de segurança. Os riscos de perdas financeiras, danos à reputação da companhia e não-atendimento a regulamentações estão entre os principais motivadores de se implementar um framework abrangente para a monitoração das principais atividades executadas por meio da infra-estrutura de TI.

Dessa forma, muito esforço tem sido empregado em:

- Mapear as vulnerabilidades dos sistemas computacionais, redes de comunicação e dados;
- Implementar e disseminar políticas e normas de segurança, código de ética, termos de compromisso etc.
- Identificar se os controles internos e programas contra fraudes são suficientes e abrangentes;
- Acumular experiência para planejar e verificar a eficácia de controles para prevenir, detectar e responder adequadamente às tentativas de fraudes;
- Reduzir o risco potencial de disputas judiciais e/ou sanções que podem surgir a partir de violações de leis ou expectativas de mercado;
- Encontrar valor prático sobre o investimento em controles internos e a necessidade de que os processos implementados sejam sustentáveis, gerenciando os riscos e mantendo a performance necessária;
- Atingir os mais altos níveis de integridade por meio de um sistema de governança de TI efetiva, controles internos adequados e transparência.

Este artigo apresenta o panorama atual dos riscos e vulnerabilidades enfrentados por grandes e médias empresas, bem como conceitos gerais de implementação de um sistema de gerenciamento dos riscos de fraudes.

Classificação das ameaças de fraudes em TI

As fraudes em TI podem ocorrer de diferentes formas, dependendo da atuação da empresa e de sua dependência tecnológica. Em geral é possível identificar dois cenários comuns a partir da origem da fraude:

Fraudes Externas – são as fraudes executadas por pessoas externas à companhia, porém utilizando recursos e sistemas da companhia. Nesta categoria encontram-se as fraudes cometidas contra sistemas de:

- Internet Banking;
- Lojas virtuais de comércio eletrônico;
- Caixas eletrônicos;
- Cartão de crédito;
- Etc.

Fraudes Internas – são as fraudes cometidas por funcionários ou colaboradores que possuem acesso às instalações da companhia e aos seus recursos computacionais internos. Aqui é possível enumerar as fraudes mais comuns ocorridas em sistemas de:

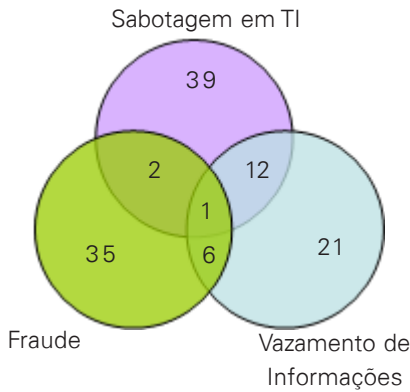
- Folha de pagamento;
- Reembolso de despesas;
- Pedidos de compra de mercadoria;
- Workflow de aprovação de limites de alçada;
- Etc.

Apesar de essa classificação ser simples e de fácil entendimento é preciso esclarecer que em muitos casos de fraudes externas existe a colaboração de funcionários internos que fornecem informações sigilosas, permitindo que a fraude seja executada. Nesse caso temos uma forma conjunta de fraude externa com vazamento de informações.

As Ameaças de Fraudes Internas

As ameaças internas podem ser materializadas sob diferentes formas e a abrangência e a consequência do ataque pode variar conforme o ramo da companhia e o objetivo do fraudador. Não é difícil encontrar na mídia relatos de casos envolvendo funcionários internos que desviaram grandes somas de dinheiro por um longo período sem que isso fosse percebido. A análise desses casos demonstra que normalmente não é preciso ter elevados conhecimentos técnicos para implementar a fraude. O conhecimento do fluxo do processo, associado com vulnerabilidades comuns de conflitos de perfil de acesso ou compartilhamento de senhas de sistemas, pode ser suficiente para gerar grandes prejuízos para companhias.

Vazamento de informações confidenciais também é um problema difícil de detectar, porque normalmente não deixa rastros e as consequências nem sempre podem ser atribuídas diretamente ao fato inicial. Por exemplo: um concorrente lança um produto muito similar alguns meses antes, porque recebeu uma informação privilegiada de que a companhia pretendia lançar tal produto que possuía grande potencial de mercado. Será muito difícil atribuir as perdas financeiras ocasionadas por esse fato a um possível vazamento de informações.



Sabotagem também é um tipo de ameaça interna que preocupa muito as companhias, uma vez que seu objetivo principal é interromper as operações da companhia. Nessa categoria, um exemplo ilustrativo são as “bombas–relógio”. Uma bomba–relógio é um programa especialmente criado por um atacante interno e colocado em ambiente de produção com o objetivo de apagar grandes quantidades de informações armazenadas em servidores de arquivos.

Um estudo realizado pela universidade americana Carnegie Mellon(*) em 2006, com 116 empresas que relataram problemas com ataques internos, demonstrou a segmentação dos incidentes nas seguintes categorias:

- 47%: sabotagem na TI
- 38%: vazamento de informações
- 34%: fraudes por meio da TI

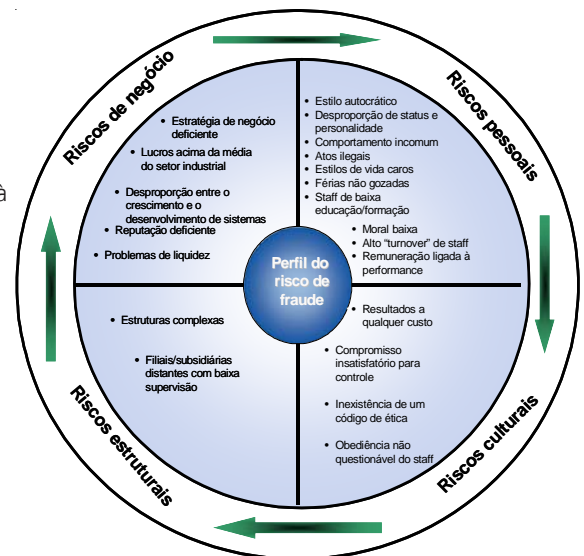
Fatores Culturais e Pessoais

Quando são analisados os casos de ataques e fraudes internas procura-se identificar quais foram os fatores motivadores. Nos casos de sabotagem na infra-estrutura de TI a maioria dos casos deve-se à ocorrência de algum evento negativo envolvendo um funcionário–chave de operação, por exemplo um administrador de sistemas. Este evento pode ocorrer em razão de sua demissão, sua transferência para outra função e sua insatisfação com aumento salarial ou bônus.

Nos casos de fraude e vazamento de informações, os fatores motivadores podem ser os mais diversos.

Entre os mais comuns destacamos os seguintes:

- Riscos Pessoais
 - Estilo autocrático
 - Moral baixa
 - Remuneração ligada à performance
- Riscos Culturais
 - Alta rotatividade de empregados
 - Resultados a qualquer custo
 - Inexistência de código de ética



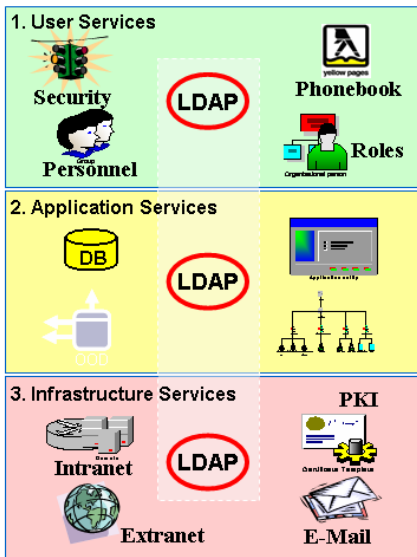
A oportunidade identificada, a partir do conhecimento de vulnerabilidades do sistema ou do processo, somada aos fatores pessoais descritos e, ainda, a percepção de falta de monitoramento que implicará a não–detecção da fraude e, conseqüentemente, impunidade incentiva o funcionário a implementar o ataque ou a fraude.

Complexidade das Técnicas Utilizadas

Em relação à análise da complexidade técnica do ataque, novamente deve-se segmentar os tipos de ataques. Conforme já descrito, normalmente os ataques de sabotagem na infra-estrutura de TI são realizados por pessoal ligado à

* Carnegie Mellon Cylab, Common Sense Guide to Prevention and Detection of Insider Threats, 2nd Edition, July 2006.

administração e operação dos sistemas. Esse pessoal tem elevada especialização técnica e grande conhecimento da arquitetura utilizada pela companhia, bem como de seus sistemas de segurança. Esse conhecimento dificulta a prevenção e detecção dos ataques desta natureza.



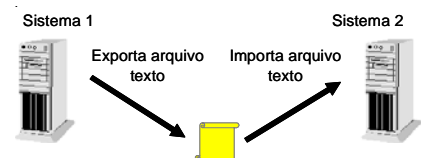
Por outro lado, o estudo das fraudes em sistemas integrados de gestão corporativos, também conhecidos como ERP – Enterprise Resource Planning, mostram que a grande maioria dos incidentes é ocasionada por deficiências na utilização de senhas de acesso à rede e aos sistemas corporativos. Algumas dessas deficiências estão enumeradas a seguir:

- Compartilhamento de senhas entre funcionários;
- Baixa complexidade na escolha das senhas;
- Contas de acesso a sistemas de funcionários demitidos ativas;
- Inexistência de processo de troca periódica de senha.

Outro problema bastante comum nos ERP é a falta de um processo de revisão dos perfis de acesso que são concedidos aos funcionários. Ao longo de sua carreira, um funcionário sofre diversas movimentações na companhia, as quais podem ser horizontais ou verticais. As horizontais são aquelas que ocorrem quando o funcionário troca de área de atuação, mas mantém o cargo. Já as verticais são aquelas nas quais ele recebe uma promoção. É fácil perceber que se não houver um processo de revisão periódico atrelado aos acessos que os funcionários possuem nos diversos sistemas da companhia, é muito provável que existam problemas de conflitos entre os acessos concedidos a funcionários. Um problema de conflito de perfil de acesso pode ser exemplificado quando um funcionário tem a possibilidade de emitir um pedido de compra e também de aprová-lo, sem nenhuma revisão adicional por outro funcionário supervisor.

Outro foco de ataque nos sistemas está na interface de conexão entre eles. Para que os sistemas possam trocar informações é necessário que eles estejam conectados de alguma forma. Existem diversas estratégias para conectar os sistemas, como por exemplo:

- Troca de arquivos;
- Utilização de um banco de dados em comum;
- Mensagens on-line etc.



Estas interfaces podem ser automatizadas ou manuais. Se a interface depender de um funcionário acionar um programa para iniciar o processo ela é caracterizada como manual. Se ela ocorrer automaticamente, sem qualquer interferência de funcionários, ela é classificada como automatizada. O problema das interfaces manuais é que, dependendo como foram concebidas, podem permitir a alteração dos dados após a exportação dos dados do primeiro sistema e antes da importação do sistema-destino. Se não houver outro controle associado ao processo, como uma reconciliação dos dados, será muito difícil detectar este tipo de fraude.

Interfaces Vulneráveis

- Interfaces manuais
- Arquivos-texto de fácil edição
- Arquivos armazenados em servidores sem controle de acesso
- Sem campos de controle

Interfaces Vulneráveis

- Interfaces automatizadas
- Transferências on-line
- Controle de integridade na importação
- Processo de conciliação
- Controle de erros

As Ameaças de Fraudes Externas

As ameaças externas têm por característica o fato de serem executadas a partir de localidades externas à companhia e contra os seus sistemas e suas aplicações.

Até há algum tempo as ameaças externas se resumiam aos ataques de adulteração das páginas Web das empresas, gerando danos de imagem e repercutindo entre as comunidades de hackers como troféus. Atualmente, diversos tipos de ameaças fazem parte das matrizes de risco das empresas. Segundo a pesquisa “2005 – E-crime Watch, Survey”, conduzida pela CSO Magazine em cooperação com o CERT e o serviço secreto americano, dos crimes eletrônicos cometidos e que foram possíveis de identificar, as empresas que participaram do estudo indicaram que enfrentaram os seguintes tipos de incidentes:

Vírus ou outro código malicioso	82%
Spyware	61%
Phishing	57%
Geração ilegal de spam	48%
Acesso não autorizado à informação, ao sistema ou à rede	43%
Ataques de negação de serviço	32%
Acesso indevido a ponto de rede sem fio	21%
Divulgação de informação privada ou confidencial	19%
Fraude	19%
Roubo de identidade	17%
Captura de senhas	16%
Roubo de propriedade intelectual	14%
“Máquinas seqüestradas” (zumbis) na rede da organização	13%
Roubo de informações	12%
Sabotagem	11%
Adulteração de página Web	9%
Extorção	2%
Outros	4%
Não sabe/não tem certeza	3%

De acordo com a pesquisa, cerca de 80% desses ataques foram realizados de forma externa à companhia.

Ataques cada vez mais sofisticados – Phishing

Atualmente os ataques estão cada vez mais sofisticados e são executados por quadrilhas bem organizadas e formadas por técnicos experientes. Para citar um caso comum à maioria dos usuários de sistemas Internet Banking vale descrever o ataque conhecido por phishing.

Nesse ataque, os fraudadores enviam milhares, talvez milhões, de e-mails para endereços adquiridos por diversas fontes. Aqui vale o comentário que existem grupos especializados em criar bases de dados de endereços de e-mail, inclusive com segmentação por tipo de banco utilizado, localização geográfica, perfil de usuário etc. Muitas vezes são utilizados métodos ilegais para a criação destas bases.

Estas mensagens contêm um programa malicioso anexado que, quando instalado na estação da vítima, passa a capturar os dados inseridos pelo usuário e os transmite para um endereço na Internet, normalmente localizado em algum país distante e de difícil comunicação, em termos de língua e acesso às autoridades locais.

A partir da instalação desse programa, quando o usuário acessa seu banco por meio da Internet, o trojan (como é chamado este programa malicioso) passa a capturar suas informações de autenticação no Internet Banking e as armazena em um servidor especialmente configurado para este fim.

Periodicamente, membros da quadrilha acessam os servidores que armazenam os dados dos clientes. Esses dados formam bases de dados completas com todas as informações necessárias para utilizar os sistemas bancários como se fossem os clientes legítimos.

A partir desse momento, essa base de dados pode ser utilizada pela quadrilha para:

- Transferir os recursos para contas de “laranjas”, permitindo o saque posteriormente;
- Realizar pagamento de contas;
- Carregar telefones celulares pré-pagos com créditos;
- Efetuar empréstimos em nome das vítimas.

A quadrilha pode ainda vender essa base, ou parte dela, para outros criminosos que, por sua vez, dependendo de sua especialidade, podem “vender os serviços” descritos.

Como os grandes bancos de varejos operam com milhões de clientes, o impacto de um ataque como esse pode ser muito significativo, tanto do ponto de vista financeiro quanto do de imagem.

Num momento em que os bancos investem grandes somas de recursos para incentivar seus clientes a migrarem das agências, cujo custo operacional é muito alto, para canais eletrônicos como os caixas eletrônicos e o próprio Internet Banking, um ataque bem implementado que trará grande repercussão entre os clientes e na própria mídia em geral pode atrapalhar esta estratégia.

Dentro desse contexto, é fundamental que as grandes empresas, assim como os bancos que utilizam a Internet como meio de interação e transação com clientes e parceiros, invistam em tecnologias e processos de segurança que minimizem as possibilidades de fraude.

A evolução dos mecanismos de segurança

Acompanhando a sofisticação dos ataques, as empresas de segurança têm buscado soluções criativas e inovadoras para dificultar a ação dos criminosos e desestimular funcionários internos a tentarem realizar fraudes eletrônicas.

Em razão dos crescentes ataques provenientes da Internet, os mecanismos de segurança de perímetro de rede evoluíram rapidamente. O perímetro de rede compõe as diversas interfaces da rede interna da companhia com:

- a Internet;
- a rede de parceiros ou clientes;
- as redes sem fio (wireless);
- os acessos de conexão remota, etc.

Esses mecanismos são formados por diferentes tecnologias como: firewalls, IDS (Intrusion Detection System), VPN (Virtual Private Network), IPS (Intrusion Prevention System), entre outros.

Com o perímetro relativamente bem protegido, o foco dos ataques tem sido as aplicações disponibilizadas pelas empresas a partir da Internet, tais como:

- Sistemas Internet Banking;
- Sistemas de lojas virtuais;
- Sistemas de consulta a exames médicos etc.

Como os mecanismos de autenticação normalmente utilizados não são suficientes para assegurar a confidencialidade das informações dos clientes, novos dispositivos estão sendo integrados a esses sistemas; entre eles destacamos:



- Dois ou três parâmetros de autenticação (senha, dados pessoais, combinação de letras etc.);
- Utilização de teclado virtual para fornecimento da senha;
- Utilização de dispositivo gerador de senhas aleatórias (Token);
- Gerador de senhas aleatórias no telefone celular;
- Cartão impresso com senhas aleatórias;
- Smartcard;
- Certificação digital do usuário (e-CPF, e-CNPJ);
- Biometria etc.

Com o maior rigor de segurança, a usabilidade dos sistemas fica evidentemente prejudicada, exigindo das empresas investimento em treinamentos on-line e elaboração de manuais para os clientes e usuários em geral.

A fraude em TI pode ser evitada?

A fraude implementada por meio de recursos de Tecnologia da Informação tem crescido gradativamente e exige o aprimoramento dos controles internos e processos de monitoramento.

Como a tecnologia evolui muito rapidamente, trazendo diversos benefícios para as áreas de negócio, e as empresas não podem deixar de implementar as novas tecnologias por motivos de competitividade e eficiência operacional, é bastante difícil afirmar que vulnerabilidades e falhas deixarão de existir nos sistemas e nas redes de computadores.

Isso não quer dizer que as fraudes em TI não possam ser evitadas ou, pelo menos, o seu risco minimizado em níveis aceitáveis pelas organizações. Para atingir esse objetivo, é necessário um esforço integrado de investimento, tanto em mecanismos de segurança tecnológica quanto em processos operacionais.

De acordo com a pesquisa “2005 – E-crime Watch Survey”, as seguintes ações foram implementadas pelas empresas que participaram do estudo com o objetivo de minimizar o risco de fraude e ataques por meio da TI:

Treinamento de segurança para novos funcionários	80%
Comunicação freqüente da administração sobre segurança	80%
Programas de treinamento e conscientização de funcionários	78%
Assinatura de termos de concordância com políticas corporativas	74%
Segregação de funções	73%
Políticas de gerenciamento de contas e senhas	72%
Incluir requisitos de segurança em negociações de contratos com fornecedores	72%
Política formal de tratamento quanto ao uso inadequado	70%
Política de segurança corporative	69%

Contratação de um CSO ou CISO	67%
Reporte obrigatório para administração de mau uso ou abuso realizado por funcionários ou terceiro	66%
Auditorias de segurança aleatórias	61%
Revisão de antecedentes de empregados ou terceiros	60%
Governança sobre as permissões de segurança	58%
Monitoramento de empregados	57%
Armazenamento e revisão de arquivos e e-mails	56%
Monitoramento de conexões da Internet	52%
Executar auditorias regulares de segurança	51%
Avaliação de riscos periódica	51%
Testes de invasão periódicos	48%
Utilização de serviços de hackers éticos	46%
Utilização de um time de resposta a incidentes	42%

Concluimos que para administrar e minimizar os impactos de fraudes e ataques é necessário que as empresas desenvolvam internamente a disciplina de gerenciamento contínuo dos riscos de fraude e que, a partir desses, direcionem os investimentos em TI e os processos operacionais.



Uma Abordagem para o Gerenciamento de Risco de Fraude

Objetivos-chave: Prevenção, Detecção e Resposta

Uma abordagem efetiva, direcionada à fraude em negócios e gerenciamento de risco e má-conduta, é uma abordagem que é focada em três objetivos:

- **Prevenção:** controles projetados para reduzir o risco de ocorrer fraude e má-conduta.
- **Detecção:** controles projetados para descobrir fraude e má-conduta quando estes ocorrerem.
- **Resposta:** controles projetados para tomar ação corretiva e remediar os danos causados por fraude e má-conduta.

Colocando tudo isso junto

Da mesma maneira como há várias formas de fraude e má-conduta em uma companhia, há várias opções de critérios de controles que os órgãos regulatórios requerem que as companhias adotem. O desafio para as companhias, então, é adotar uma abordagem compreensiva e integrada que leve em consideração todos os aspectos relevantes e permita que estes aspectos trabalhem em conjunto. Sendo assim, é evitado o esforço duplicado e a fragmentação de recursos.

Esta tarefa começa com o entendimento de todas as várias estruturas de controles e critérios que se aplicam às companhias (veja figura 2). Quando esta categorização é completa, a organização tem as informações de que necessita para criar um programa compreensivo no qual os elementos de prevenção, detecção e resposta podem ser integrados e gerenciados.

Figura 2: Padrões internacionais selecionados

Jurisdição	Estrutura	Relevância
Austrália	Corporations Act 2001 (incluindo adições da CLERP 9)	Tem por objetivo fortalecer a estrutura das demonstrações financeiras.
Canadá	The Multilateral Instrument 52-109	Promove uma “cultura de controle interno” para uma melhoria da qualidade das demonstrações financeiras no Canadá.
Holanda	Corporate Governance Code of Conduct 2004	Busca aprimorar a transparência nas relações entre os acionistas e a gerência e também aprimorar a estrutura e a contabilidade em gerenciamento na Holanda.
Reino Unido	The Companies Act 2004	Tem por objetivo aumentar a confiança nas demonstrações financeiras e a independência de auditores e regulamentações de auditoria no Reino Unido.
Estados Unidos	Sarbanes-Oxley Act of 2002	Introduziu mudanças substanciais na governança corporativa e requisições financeiras de organizações registradas na SEC e listadas no ‘U.S. Stock exchanges’.



Fonte: KPMG LLP (U.S.), 2006.

A figura 3 apresenta exemplos de elementos de um programa compreensivo estruturado para responder à fraude, preveni-la e detectá-la.

Figura 3: Exemplo de Elementos do programa antifraude

Prevenção	Detecção	Resposta
Comitê de auditoria de supervisão Funções executivas e de gerenciamento Auditoria Interna, compliance e funções de monitoramento		
– Avaliação do risco de fraude e má-conduta – Código de conduta e padrões relacionados – Obrigações de empregados e terceiros – Comunicação e treinamento – Processo específico de controles de risco de fraude	– Mecanismos de alerta – Auditoria e monitoramento – Análise judicial e proativa de dados – Procedimentos para descobertas – Procedimentos para ação corretiva	– Procedimentos de investigação interna – Procedimentos de mensuração e repressão



Prevenção

Controles preventivos são projetados para ajudar a reduzir o risco de ocorrer fraude e má-conduta.

Liderança e Governança

Supervisão do comitê de auditoria

O comitê de auditoria de uma empresa desempenha um papel importante na supervisão e implementação de controles para minimizar o risco de fraude e má-conduta. O comitê e a administração são responsáveis por tornar claras suas regras e garantir que o suporte institucional é estabelecido nos mais altos níveis para práticas de negócios éticas e responsáveis.

O comitê não tem apenas o dever de garantir que a organização tenha programas e controles para abordar o risco de práticas inadequadas, mas também tem o dever de garantir que estes controles sejam efetivos.

Como uma medida prática, o comitê pode delegar o papel principal de vigilância e gerenciamento de risco de fraude e má-conduta para a auditoria (auditoria típica), que entre suas tarefas inclui:

- Revisão e discussão de assuntos levantados durante a avaliação de fraude e má-conduta na entidade.
- Revisar e discutir com os auditores internos e externos os resultados da qualidade dos programas e controles antifraude da organização.
- Estabelecer procedimentos para o recebimento e tratamento de questões ou preocupações relacionadas à contabilidade questionável ou aos assuntos de auditoria.

Uma estratégia robusta de fraude é aquela patrocinada pelo mais alto nível da administração, firme e enraizada na cultura. Ameaças de fraude são dinâmicas e fraudadores constantemente desenvolvem novas técnicas para explorar o alvo mais fácil.

Philip Robinson
Líder do setor de crime financeiro,
Autoridade em serviços financeiros

Alcançar uma boa governança corporativa não é apenas responsabilidade dos diretores, investidores e reguladores; deve ser um objetivo principal da alta administração. Uma governança corporativa deficiente enfraquece o potencial da companhia e, no pior dos casos, pode ocasionar dificuldades financeiras e até mesmo fraude.

Bill Witherell
Diretor de finanças e assuntos empresariais
Organização para Cooperação econômica e desenvolvimento
Estratégias de CFO: Fórum de Contabilidade Corporativa 2004, 17 de Maio de 2004

Supervisão da alta administração

Para ajudar a garantir que controles de fraude e má-conduta permaneçam efetivos e em harmonia com os padrões governamentais, a responsabilidade da abordagem de gerenciamento de risco e má-conduta da organização deve ser dividida nos níveis mais altos (exemplo: indivíduos com controle ou papel substancial na criação de políticas). Esta supervisão começa com a prevenção e também precisa fazer parte dos esforços para detecção e resposta.

O CEO tem a posição ideal para influenciar as ações dos funcionários por meio de sua liderança, especificamente por mostrar o nível ético da organização, e um papel crucial em encorajar uma cultura de ética e integridade. O CEO pode liderar pelo exemplo, disponibilizando recursos para esforços antifraude e colocando a alta administração como responsável por violações de conformidade.

A responsabilidade por esforços antifraude deve permanecer com um líder sênior, muitas vezes um compliance officer (oficial de conformidade) que trabalha com a equipe de auditoria interna e os especialistas em assuntos relacionados. O compliance officer é responsável por coordenar a abordagem da organização quanto à prevenção, detecção e resposta à fraude e má-conduta. Quando assuntos relacionados à fraude e má-conduta são levantados, este profissional pode alocar os recursos corretos para lidar com o problema e fazer mudanças operacionais necessárias. O compliance officer pode também presidir um comitê de gerentes de diferentes funções, que:

- Coordenam os esforços de avaliação de risco da organização.
- Estabelecem políticas e padrões de práticas aceitáveis de negócio.
- Fiscalizam o projeto e a implementação de programas e controles antifraude.
- Comunicam os resultados das atividades de gerenciamento de risco de fraude da organização à diretoria e/ou ao comitê de auditoria.

Outros líderes de negócios, como líderes de departamentos (desenvolvimento de produtos, marketing, assuntos regulatórios e recursos humanos), também devem participar de responsabilidades dentro da estratégia antifraude da organização. Estes fiscalizam áreas de operações diárias nas quais podem surgir riscos e podem servir como especialistas em determinados assuntos para ajudar o compliance officer com respeito à sua área em particular de conhecimento e responsabilidade.

Função da Auditoria Interna

A função da auditoria interna em uma organização moderna é um elemento-chave em atividades antifraude, suportando a abordagem da administração para prevenir, detectar e responder à fraude e má-conduta. A pesquisa da KPMG realizada em 2003, a respeito de fraude, mostra que 65% das respostas indicam que fraudes foram descobertas por meio do trabalho da auditoria interna. Estas responsabilidades representam uma mudança do papel mais tradicional da auditoria interna (que é o de examinar a efetividade dos controles da entidade).

No geral, a auditoria interna deve ser responsável por:

- Planejar e conduzir a avaliação do desenho e efetividade dos controles antifraude.
- Ajudar a organização na avaliação dos riscos de fraude e ajudar a encontrar conclusões quanto a estratégias apropriadas para mitigar estes riscos.
- Comunicar o comitê de auditoria sobre a avaliação dos controles internos e das auditorias, investigações e atividades relacionadas.

Avaliação do risco de fraude e má-conduta

Todas as organizações normalmente enfrentam uma variedade de riscos de fraude e má-conduta. Uma avaliação dos riscos e má-conduta ajuda a administração a entender os riscos que são exclusivos a seu negócio, identificar falhas ou fraquezas em controles para mitigar estes riscos e desenvolver um plano prático para se direcionar os recursos e controles corretos para reduzir os riscos.

A administração deve garantir que esta avaliação seja conduzida por toda a organização, levando em consideração as unidades de negócio significativas da entidade, os processos e as contas.

Com dados fornecidos pelos donos dos controles (control owners) em relação aos riscos relevantes para alcançar os objetivos organizacionais, uma avaliação dos riscos de fraude e má-conduta inclui os passos listados na figura 4.

Figura 4: Processo de avaliação de riscos de fraude



Enquanto a administração é responsável por executar uma avaliação focada dos riscos nos processos e considerar os resultados avaliando a efetividade dos controles, o comitê de auditoria normalmente tem um papel de supervisão neste processo. O comitê de auditoria é responsável por revisar a avaliação de risco feita pela administração, garantindo que esta mantenha um esforço continuado e interaja com o auditor independente da entidade para garantir que os resultados da avaliação sejam comunicados apropriadamente.

52%

Percentagem de funcionários nos Estados Unidos que relataram que seus códigos de conduta não são levados a sério.

Pesquisa sobre Integridade realizada pela KPMG 2005 – 2006 (KPMG Forensic Integrity Survey 2005 – 2006)

Código de conduta

O código de conduta de uma organização é um dos mais importantes veículos de comunicação que a administração pode usar para comunicar a seus funcionários os padrões que definem uma conduta de negócio aceitável. Um código bem escrito e comunicado vai além de retransmitir políticas da companhia. Este código define a tônica da cultura de controles da organização, demonstrando o comprometimento da administração com a integridade e disponibilizando os recursos para ajudar os funcionários a alcançar os objetivos definidos.

Um código de conduta bem formulado normalmente inclui:

- Confirmação da liderança da organização, enfatizando o comprometimento com a integridade.
- Linguagem simples, concisa e positiva, que pode ser prontamente entendida por todos os funcionários.
- Tópicos fundamentados em cada uma das principais políticas da companhia e/ou nas áreas de risco.
- Guia prático de riscos fundamentado em cenários tangíveis ou exemplos hipotéticos.
- Um formato visual convidativo que encoraje a leitura, o uso e o entendimento.
- Ferramentas para decisão de escolhas éticas que ajudem os funcionários a fazerem as escolhas certas.
- Canais de comunicação para relatar e mecanismos viáveis que os funcionários podem usar para informar preocupações ou buscar aconselhamentos sem medo de represálias.

Eu digo que ter um código de ética que não é vigorosamente implementado é pior do que não ter um código de ética. É uma forma de hipocrisia.

Roel C. Campos
SEC (U.S. Securities and Exchange Commission,
16 de outubro de 2002

Levantamento de histórico de funcionários e terceiros

Um aspecto importante de uma estratégia efetiva de prevenção à fraude e má-conduta é o levantamento do histórico profissional/criminal na contratação, retenção e promoção de funcionários, agentes, fornecedores e outros terceiros. Esse levantamento pode ser especialmente importante para os funcionários identificados como tendo autoridade sobre o processo das demonstrações financeiras.

O escopo e a profundidade deste processo normalmente variam com base nos riscos identificados pela organização, na função de trabalho do indivíduo e/ou no nível de autoridade e nas leis específicas do país em que a organização reside.

Em certas situações, pesquisar terceiros pode ser uma escolha válida. Por exemplo, a administração pode querer avaliar agentes, consultores ou trabalhadores temporários que podem acessar informações confidenciais.

A análise do histórico do profissional tem seu início no começo de um processo de contratação ou relação de negócios e continua daí em diante. Por exemplo, levar em conta considerações sobre comportamento, como aderência aos principais valores da organização por meio de avaliações de desempenho, fornece um indicador de que a administração não se importa apenas com os objetivos que o funcionário alcança, mas também que estas conquistas foram alcançadas de uma maneira consistente com os valores e princípios da companhia.

49%

Percentagem de funcionários nos Estados Unidos que relataram que seriam recompensados de acordo com seus resultados e não pelos meios usados para alcançá-los.

Pesquisa sobre Integridade realizada pela KPMG 2005 – 2006 (KPMG Forensic Integrity Survey 2005 – 2006)

55%

Percentagem de funcionários nos Estados Unidos que relataram que não possuíam conhecimento suficiente dos padrões de conduta que se aplicam a suas tarefas.

Pesquisa sobre Integridade realizada pela KPMG 2005 – 2006 (KPMG Forensic Integrity Survey 2005 – 2006)

Comunicação e treinamento

Tornar os funcionários cientes de suas obrigações no que diz respeito à fraude e má-conduta começa com comunicação e treinamento. Enquanto muitas organizações comunicam estes assuntos de maneira direta, esforços feitos sem planejamento e priorização podem falhar em prover aos funcionários uma mensagem clara de que suas responsabilidades devem ser observadas seriamente.

Na formulação de um plano de comunicação e treinamento, a administração deve considerar o desenvolvimento iniciativas de conscientização sobre fraude e má-conduta, que são:

- Compreensíveis e fundamentadas nas funções de trabalho e áreas de riscos.
- Integradas com outros treinamentos, sempre que possível.
- Efetivas em vários ambientes, usando múltiplos métodos e técnicas.
- Regulares e freqüentes, cobrindo uma parte relevante dos funcionários.

A alta administração precisa mudar o seu pensamento de conformidade como primariamente um centro de custo para a consideração dos benefícios da conformidade em proteger contra os riscos legais e de reputação que podem ter um impacto no lucro final.

*Susan Schmidt Bies
U.S. Federal Reserve Board Governor
The Bank Administration Institute's Fiduciary Risk Management Conference 2004
Assuntos atuais sobre Governança Corporativa
26 de abril de 2004*

Detecção

Controles para detecção são projetados para descobrir fraude e má-conduta quando estes ocorrem.



Mecanismos de busca de aconselhamento e denúncia de má-conduta

Com a supervisão e direção da alta administração, as organizações tendem a prover múltiplos canais para relatos de preocupações sobre fraude e má-conduta aos funcionários. Muitos normalmente requerem que os funcionários sigam um processo que se inicia com o alerta aos próprios gerentes ou alguém responsável por isso na área de Recursos Humanos ou compliance officer. Linhas especiais de telefone (Hotline) são comumente disponibilizadas e podem ser usadas a qualquer momento, embora estas sejam normalmente para uso quando os canais normais de comunicação não são práticos ou efetivos. Os sistemas de Hotline normalmente provêem um método viável por meio do qual funcionários e terceiros são encorajados a:

- Comunicar preocupações sobre fraudes em potencial e má-conduta, incluindo contabilizações e assuntos questionáveis de auditoria.
- Buscar aconselhamento antes de tomar decisões quando a maneira correta de fazê-lo não for clara.

Um sistema de Hotline bem projetado normalmente inclui as seguintes características:

- **Confidencialidade.** Todos os assuntos relatados por meio do Hotline são tratados confidencialmente. Os operadores informam aos usuários que suas preocupações serão relatadas apenas em uma base de "saber o necessário"

e que medidas de segurança estão em vigor para garantir que esta confidencialidade seja mantida. Os operadores das linhas notificam os usuários se a confidencialidade a respeito do assunto está sujeita a limitações judiciais.

- **Anonimato.** Os procedimentos da organização permitem a submissão e execução de ligações anônimas. Por exemplo, usuários que desejam permanecer em anonimato recebem um número para rastrear o caso, por meio do qual estes podem prover detalhes adicionais relacionados ao seu caso ou alegação e/ou checar o status ou o resultado de sua ligação/denúncia.
- **Ampla disponibilidade da organização.** Funcionários em localizações internacionais podem utilizar o Hotline para relatos por meio de dispositivos como URA e roteamento de ligações sem custos.
- **Assistência em “tempo real!”** O Hotline é designado para prover um atendimento imediato e ao vivo de uma chamada, para facilitar um atendimento consistente de uma questão levantada ou preocupação e também para prover orientação imediata. Dessa forma, operadores de Hotlines precisam ser apropriadamente qualificados, treinados e, em algumas situações, autorizados a dar aconselhamentos.
- **Procedimentos de gerenciamento de dados.** Os operadores usam procedimentos consistentes para colher fatos relevantes e gerenciar as ligações recebidas.
- **Classificação de riscos relacionados às demonstrações financeiras.** Os Hotlines incluem procedimentos segundo os quais indivíduos qualificados (exemplo: auditor interno, profissionais relativos à lei e à segurança) podem determinar se a natureza de uma declaração pode gerar um risco para as demonstrações financeiras.
- **Notificação do comitê de auditoria.** Os Hotlines incluem procedimentos que especificam a natureza das declarações recebidas que devam ser levadas ao comitê de auditoria.
- **Acompanhamento da não-retaliação.** Os procedimentos da organização permitem o acompanhamento com funcionários periodicamente após o caso denunciado por telefone ter sido fechado (exemplo: acompanhamento em intervalos de um, três e seis meses) para garantir que funcionários que fizeram denúncias não sofreram retaliação. A companhia encoraja os funcionários a denunciar qualquer tipo de retaliação e toma medidas imediatas contra quem retalia.
- **Comunicações importantes.** A organização publica a existência de um sistema de Hotline de forma destacada. Tal comunicação pode incluir, entre outros, (i) descrever o Hotline no código de conduta e em outras publicações-chave da companhia e em treinamentos; (ii) colocar os números das linhas em pôsteres, faixas, cartões, protetores de tela, listas telefônicas ou calendários de mesa; e (iii) comunicar minicursos de estudos fundamentados em ligações telefônicas para funcionários (exemplo: boletim informativo, programas de treinamento ou sites na Intranet) para demonstrar que a organização valoriza ligações feitas para o Hotline e que está pronta a prover assistência àqueles que usam esta linha.

33%

Percentagem de funcionários na Austrália/Nova Zelândia que relataram que avisos iniciais de problemas de fraude foram ignorados.

Pesquisa sobre fraude feita pela KPMG 2004

Auditoria e Monitoramento

Sistemas de auditoria e monitoramento que são projetados de modo aceitável a detectar fraude e má-conduta são ferramentas importantes que a administração pode usar para determinar se os controles de uma organização estão funcionando como o pretendido. Como é impossível fazer auditoria de todo risco de fraude e má-conduta, a administração deve desenvolver um plano compreensivo de auditoria e monitoramento que é fundamentado em riscos identificados por meio do processo de avaliação de riscos feito pela organização.

Um plano de auditoria e monitoramento deve então abranger atividades que são ligadas, a fundo, à natureza e ao grau do risco envolvido, com assuntos de maior risco recebendo tratamento prioritário. Atividades de auditoria (uma avaliação de eventos passados) e monitoramento de atividades (uma avaliação conduzida em tempo real) devem ser executadas, mas não limitadas às seguintes áreas nas quais:

- Há preocupações específicas quanto a um procedimento, conta ou posição-chave.
- A companhia tem um histórico de fraude e má-conduta.
- Há uma grande rotatividade de funcionários ou mudanças organizacionais.
- Leis e regulamentações têm mudado significativamente.
- Auditorias são requeridas legalmente, ou agências governamentais estão visando a ações de verificação de conformidade.

Gerentes de uma organização envolvidos nos esforços de auditoria e monitoramento devem não apenas ter suficiente treinamento e experiência, mas também a capacidade de avaliar os controles pelos quais são responsáveis de forma independente. Da forma mais eficiente, os procedimentos de auditoria e monitoramento devem:

- Ocorrer no curso normal das operações, incluindo as atividades de gerenciamento regular e supervisão.
- Buscar informações externas para confirmar informações obtidas internamente.
- Comunicar oficialmente a alta administração sobre as deficiências e exceções identificadas, para que o dano à organização seja apropriadamente entendido e mitigado.
- Usar os resultados para melhorar e modificar outros controles, como comunicações e treinamento, avaliações de desempenho e disciplina.

Análise proativa de dados

Muitos dos indicadores de fraude e má-conduta, ambos reais e potenciais, residem nos dados financeiros, operacionais e de transações de uma organização e podem ser identificados utilizando ferramentas e técnicas de análise de dados. Essa análise proativa de dados usa sofisticados testes analíticos, comparação de dados por computador e identificador de relações não-óbvias para destacar potenciais fraudes ou má-conduta que podem permanecer sem o conhecimento da administração por anos. Os benefícios dessa análise podem incluir, entre outros:

- Identificação de relações escondidas entre pessoas, organizações e eventos.
- Um meio para analisar transações suspeitas.
- Habilidade para avaliar a efetividade dos controles internos designados para prevenir ou detectar atividades fraudulentas.
- Monitoramento contínuo de ameaças de fraude e vulnerabilidades.
- Habilidade de considerar e analisar milhares de transações em pouco tempo, mais eficientemente, e com melhor custo-benefício do que usando-se técnicas de amostras mais tradicionais.

As transações podem ser analisadas utilizando monitoramento retrospectivo ou contínuo das transações. A análise retrospectiva permite às organizações analisarem transações em incrementos de um ou dois anos, capacitando-as a obter padrões que não são visíveis em análises de curto prazo. Pela criação da capacidade de executar análise proativa com base em dados retroativos, incluem-se passos para:

- Avaliar o perfil de risco de fraude de sistemas ou processos.
- Definir os objetivos gerais da análise.
- Criar uma metodologia para adquirir, extrair e avaliar os dados.
- Definir a análise a ser executada.
- Selecionar ferramentas de programas de computador a serem usadas na realização destes testes.
- Realizar a análise, agregar e priorizar os resultados, rever e solucionar as exceções identificadas.

Diferente da análise retrospectiva, a monitoração contínua das transações permite à organização identificar transações potencialmente fraudulentas em, por exemplo, uma base diária, semanal ou mensal. Organizações freqüentemente usam a monitoração contínua para analisar áreas que possuem particularmente altos riscos.



Resposta

Controles de resposta são projetados para tomar ação corretiva e remediar os danos causados pela fraude ou má-conduta.

Investigações

Quando informações relacionadas a reais ou potenciais fraudes e má-conduta são descobertas, a administração deve se preparar para conduzir uma investigação interna objetiva e abrangente. O objetivo dessa investigação é colher fatos que levem a uma avaliação da suspeita de violação, para que a administração possa decidir por um sólido plano de ação.

Pela condução de uma efetiva investigação interna, a administração pode deparar-se com uma situação problemática e ter a oportunidade de evitar uma investigação governamental. Um processo investigativo bem projetado irá normalmente incluir os seguintes atributos, entre outros:

- Supervisão pelo comitê de auditoria da organização, ou um comitê especial, ambos que contenham integrantes independentes que sejam capazes de impedir pressão indevida ou interferência da administração.
- Direção de um conselho externo, selecionado pelo comitê de auditoria, com pouca ou nenhuma ligação com a equipe de administração da entidade e que possa executar uma investigação imparcial, independente e qualificada.
- Verificação da auditoria externa da organização para que o processo possa estar de acordo com o escopo de trabalho proposto na auditoria das demonstrações financeiras da organização.
- Requerimento de cooperação total, não permitindo que nenhum funcionário ou membro da gerência possa omitir fatos que deram início à investigação.
- Procedimentos para relatórios, provendo informações relevantes às descobertas da investigação aos auditores externos e reguladores e, quando necessário, ao público em um espírito de cooperação e transparência.

Com base em vários fatores, incluindo a natureza do ato ilegal em potencial, as partes relacionadas e a materialidade, a organização pode decidir usar um ou mais dos passos citados. A administração deve consultar as áreas de supervisão e seus procedimentos internos para determinar os passos que melhor se adaptam à alegação.

Responsabilidades e Punições

Um sistema de disciplina confiável e consistente é um controle-chave que pode ser efetivo em dissuadir fraude e má-conduta. Disciplina apropriada é adicionalmente um requerimento de estrutura de regulamentos de liderança. Determinando punições exemplares, a administração envia mensagens interna e externa de que a organização trata com prioridade o gerenciamento de risco de fraude e má-conduta.

Um processo de punições bem projetado será comunicado a todos os funcionários e inclui direções que abrangem toda a companhia e promovem:

- Punições consistentes e progressivas de acordo com a natureza e seriedade da ofensa (exemplo: aviso oral, aviso por escrito, suspensão, redução de pagamento, transferência de local, rebaixamento de posição ou desligamento da organização).
- Aplicação consistente e uniforme de disciplina, independentemente de nível, tempo de cargo ou tipo de função.

47%

Percentagem de funcionários nos Estados Unidos que informaram que contraven-tores seriam punidos justamente, independentemente de sua posição.

Pesquisa sobre Integridade realizada pela KPMG 2005 – 2006 (KPMG Forensic Integrity Survey 2005 – 2006)

Responsabilizar os gerentes pela má-conduta de seus subordinados é outra importante consideração. Gerentes podem ser punidos nos casos em que estes sabiam, ou deveriam saber, que fraude ou má-conduta poderia estar acontecendo, ou quando:

- Direcionaram ou pressionaram outros a violar os padrões da companhia para alcançar objetivos de negócios ou definiram objetivos irrealistas que levaram ao mesmo efeito.
- Falharam em garantir que os funcionários recebessem treinamento ou recursos adequados.
- Falharam em dar um exemplo positivo de atuação com integridade ou tiveram algum acontecimento anterior de não perceber/permitir violações.
- Forçaram o atendimento aos padrões da companhia de maneira inconsistente ou retaliaram outros por terem relatado suas preocupações.

Ação Corretiva

Uma vez que a fraude ou má-conduta tenha ocorrido, a administração deve tomar ações para remediar os danos causados, considerando, por exemplo, as medidas a seguir:

- Voluntariamente revelar os resultados da investigação ao governo ou a outra entidade relevante (como um regulador).
- Consertar os danos causados.
- Examinar a origem da causa da falha dos controles, garantindo que o risco seja mitigado e que os controles sejam reforçados.
- Administrar punições aos envolvidos nas ações inapropriadas e também aos que são da gerência.
- Comunicar aos funcionários em geral que a administração tomou medidas apropriadas e responsivas.

Embora uma divulgação pública de fraude ou má-conduta possa ser constrangedora para uma organização, a administração deve mesmo assim considerar esta ação no sentido de combater ou evitar publicidade negativa, demonstrando boa-fé e ajudando a finalizar o assunto.

Tradução parcial da publicação *Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response*, da KPMG Forensic, 2006, realizada por Frank Meylan, Sócio de IRM – Information Risk Management

63%

Percentagem de organizações Australianas/e da Nova Zelândia que relataram o incidente à polícia.

Pesquisa sobre fraude feita pela KPMG 2004

Contatos

Pedro Melo, Sócio
Sidney T. Ito, Sócio
André Coutinho, Sócio
Irani Ugarelli, Diretora

Tel. (11) 2183-3000
e-Mail: acibrasil@kpmg.com.br

Todas as informações apresentadas neste documento [ou inserir o nome da publicação, do informativo ou de outro material que esteja sendo remetido] são de natureza genérica e não têm por finalidade abordar as circunstâncias de nenhum indivíduo específico ou entidade. Embora tenhamos nos empenhado em prestar informações precisas e atualizadas, não há nenhuma garantia de sua exatidão na data em que forem recebidas nem de que tal exatidão permanecerá no futuro. Essas informações não devem servir de base para se empreender qualquer ação sem orientação profissional qualificada, precedida de um exame minucioso da situação em pauta.

O *Audit Committee Institute* é uma iniciativa imparcial e independente da KPMG.

© 2007 KPMG Auditores Independentes, uma sociedade brasileira e firma-membro da rede KPMG de firmas-membro independentes e afiliadas à KPMG International, uma cooperativa suíça. Todos os direitos reservados. Impresso no Brasil.

O nome KPMG e o logotipo KPMG são marcas comerciais registradas da KPMG International, uma cooperativa suíça.