IPPF - GUIAS PRÁTICOS

AUDITORIA INTERNA E FRAUDE

Instituto dos Auditores Internos do Brasil

Índice

Introdução

O propósito deste Guia Prático é aumentar a consciência do auditor interno com relação à fraude e oferecer orientações sobre como abordar riscos de fraude em trabalhos de auditoria interna.

A Estrutura Internacional de Práticas Profissionais (IPPF) define as seguintes *Normas Internacionais para Prática Profissional de Auditoria Interna* (*Normas*) com relação à fraude e ao papel do auditor interno em detectar, prevenir e monitorar riscos de fraude e abordar estes riscos em auditorias e investigações.

Norma 1200 do IIA: Proficiência e Zelo Profissional Devido

1210.A2 – Os auditores internos devem possuir conhecimento suficiente para avaliar o risco de fraude e como este é gerenciado pela organização; porém não se espera que possuam a especialização de uma pessoa cuja principal responsabilidade seja detectar e investigar fraudes.

Norma 1220 do IIA: Zelo Profissional Devido

1220.A1 – Os auditores internos devem exercer o zelo profissional devido, levando em consideração:

- A extensão do trabalho necessária para alcançar os objetivos do trabalho de auditoria;
- A complexidade relativa, a materialidade ou a significância dos assuntos aos quais os procedimentos de avaliação (*assurance*) são aplicados;
- A adequação e a eficácia dos processos de governança, gerenciamento de riscos e controles;
- A probabilidade de erros significativos, fraudes ou não conformidades; e
- O custo da avaliação (*assurance*), em relação aos benefícios em potencial.

Norma 2060 do IIA: Reporte à Alta Administração e ao Conselho

O diretor executivo de auditoria deve reportar periodicamente à alta administração e ao conselho sobre o propósito, a autoridade e a responsabilidade da atividade de auditoria interna e o desempenho em relação ao seu planejamento. Os reportes devem também incluir a exposição de pontos de riscos significativos e de controles, incluindo os riscos de fraude, os assuntos de governança e outros assuntos necessários ou solicitados pela alta administração e pelo conselho.

Norma 2120 do IIA: Gerenciamento de Riscos

2120.A2 – A atividade de auditoria interna deve avaliar o potencial de ocorrência de fraude e como a organização gerencia o risco de fraude.

Norma 2210 do IIA: Objetivos do Trabalho de Auditoria

2210.A2 – Os auditores internos devem considerar a probabilidade de erros significativos, fraudes, não conformidades e outras exposições ao desenvolver os objetivos do trabalho.

Além disso, consulte o Anexo A – Material de Referência, que lista as Práticas Recomendadas da IPPF que abordam fraude.

Sumário Executivo

A fraude impacta as organizações negativamente de muitas formas, inclusive com implicações financeiras, de reputação, psicológicas e sociais. De acordo com inúmeras pesquisas, as perdas monetárias por conta da fraude são significantes. No entanto, o custo total da fraude é incomensurável em termos de tempo, produtividade e reputação, incluindo as relações com clientes. Dependendo da severidade da perda, as organizações podem ser prejudicadas de forma irreparável, por conta do impacto financeiro da atividade de fraude. Portanto, é importante que as organizações tenham um programa forte contra fraude, que inclua programas de conscientização, prevenção e detecção, assim como um processo de avaliação do risco de fraude para identificar tais riscos, dentro da organização.

As fraudes podem ser cometidas por um funcionário de qualquer nível da organização, como também por aqueles externos à organização. Há três características comuns na maioria das fraudes:

- Pressão ou incentivo – a necessidade que o fraudador está tentando satisfazer ao cometer a fraude.
- Oportunidade – a habilidade do fraudador de cometer a fraude.
- Racionalização – a habilidade do fraudador de justificar a fraude em sua mente.

Um programa eficaz de gerenciamento de fraude inclui:

- Política de Ética da Empresa – o "tom no topo" a partir da alta administração.
- Consciência de Fraude – entender a natureza, as causas e as características da fraude.
- Avaliação de riscos de fraude – avaliar o risco dos diversos tipos de fraude.
- Revisões contínuas – uma atividade de auditoria interna que considera o risco de fraude em toda auditoria e conduz os procedimentos apropriados, com base no risco de fraude.
- Prevenção e detecção – esforços para reduzir a ocorrência de oportunidades de fraude e persuadir os indivíduos a não cometer fraude por conta da probabilidade de detecção e punição.
- Investigação – procedimentos e recursos para investigar a fundo e reportar um evento suspeito de fraude.

Uma atividade eficaz de auditoria interna pode ser de grande ajuda para lidar com a fraude. Embora a gerência e o conselho sejam, no final das contas, os responsáveis pela dissuasão de fraude, os auditores internos podem auxiliar a gerência a determinar se a organização tem os controles internos adequados e se promove um ambiente de controle adequado.

Há diversas abordagens que o DEA pode usar para considerar a fraude na condução das atividades de auditoria interna:

- Auditoria dos controles da gerência sobre a fraude. Isso inclui políticas, práticas de conscientização, o *tone at the top*, a governança do conselho e da alta administração (o ambiente de controle), assim como práticas relacionadas, como avaliações de riscos, estimar a adequação dos controles de prevenção e detecção no gerenciamento do risco de fraude dentro da tolerância da organização, gestão de incidentes, investigações e práticas de recuperação. A auditoria interna deve alocar recursos para as atividades relacionadas à fraude, de acordo com a proporção entre o risco de fraude e os demais riscos organizacionais.

- Auditoria para detectar possíveis fraudes testando processos de alto risco, com a intenção de buscar indicadores de fraude, dentro da organização e em relações externas de negócios. Por exemplo, testar a folha de pagamento em busca de funcionários fantasmas ou verificar as faturas de fornecedores em busca de superfaturamento, comparar os endereços dos fornecedores com os endereços dos funcionários para detectar fornecedores fictícios ou revisar bases de dados em busca de transações em duplicidade.

- Considerar a fraude como parte de toda auditoria. Por exemplo, fazer um brainstorming sobre o risco de fraude, avaliar os controles de fraude, desenvolver procedimentos que considerem o risco de fraude ou avaliar erros para determinar se poderiam ser indicadores de fraude. Os resultados cumulativos podem pôr em perspectiva se a consciência da gerência e seus programas de gerenciamento de riscos foram implementados com eficácia, em toda a organização.

- Consultar tarefas ajuda a gerência a identificar e avaliar riscos e determinar a adequação do ambiente de controle para revisões de processos, novas iniciativas de negócio ou aplicativos de TI. A facilitação da autoavaliação da gerência é um outro exemplo de avaliação do risco de fraude, garantindo que os controles estejam em prática para mitigar estes riscos e determinando quem monitora os resultados.

Este documento discutirá a fraude e oferecerá orientações gerais para ajudar os auditores internos a atingirem a conformidade com as *Normas* profissionais. Para aprender mais sobre a detecção e controle de fraude, leia o Anexo A – Material de Referência.

Definição de Fraude

A fraude engloba uma grande variedade de irregularidades e atos ilegais caracterizados pelo engano ou representação enganosa intencional. A IPPF do *The Institute of Internal Auditors* define *fraude* como:

"Quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam no uso de ameaça de violência ou de força física. As fraudes são perpetradas por partes e organizações a fim de se obter dinheiro, propriedade ou serviços; para evitar pagamento ou perda de serviços; ou ainda para garantir vantagem pessoal ou em negócios."

Outra definição de fraude, tirada da publicação "*Managing the Business Risk of Fraud: A Practical Guide*", patrocinada pelo *The IIA*, pelo *American Institute of Certified Public Accountants* e pela *Association of Certified Fraud Examiners*, declara que:

"Fraude é qualquer ato ou omissão intencional para enganar outros, levando a vítima a sofrer uma perda e/ou o feitor a ter um ganho."

Fraudes são caracterizadas pelo engano intencional ou pela representação enganosa. Este guia prático pode se referir como "fraude" a certas ações que também podem ser definidas legalmente e/ou conhecidas comumente como *corrupção*.

Conscientização contra Fraude

Níveis crescentes de fraude, um ambiente de elevada regulação e questões apontadas por auditores internos e externos e por conselhos de administração fizeram com que as empresas aumentassem a vigilância em seus esforços contra a fraude. Mesmo em meio a uma cultura de maior conscientização, uma organização pode ser vítima de fraude e ainda não estar ciente dessa realidade. Esquemas fraudulentos são frequentemente crimes contínuos que podem durar meses ou até mesmo anos, antes que sejam detectados, o que torna difícil a mensuração das perdas associadas à fraude. As perdas por fraude que são conhecidas e confirmadas deixam claro seu alto custo. O verdadeiro custo da fraude, no entanto, é ainda maior do que apenas a perda de dinheiro, considerando seu impacto no tempo, produtividade, reputação e relacionamento com o cliente.

Corrupção – o mau uso do poder confiado a alguém para ganhos particulares – e a fraude têm impactado adversamente inúmeras organizações. O alto custo da governança corporativa, multas associadas e penalidades foram um resultado direto das fraudes corporativas. Executivos de negócios envolvidos em litígio e, em circunstâncias extremas, foram condenados à prisão quando suas operações globais não estiveram em conformidade com os requisitos legais e regulatórios.

A fraude impacta negativamente as organizações de formas diferentes, incluindo financeiramente, psicologicamente, socialmente e ainda suas reputações. Organizações vêm sendo forçadas a fechar suas operações por conta do impacto dos danos financeiros e de reputação e os efeitos psicológicos e sociais vêm sendo especialmente devastadores para os funcionários dessas empresas. As vítimas da fraude também sofrem danos mentais e emocionais e efeitos físicos relacionados ao estresse, além de suas perdas financeiras. As vítimas sentem que roubaram não apenas seu dinheiro, mas sua segurança, autoestima e dignidade. No final das contas, a fraude não verificada pode ser prejudicial para qualquer empresa.

A fraude varia de pequenos roubos de funcionários e comportamento improdutivo, até a apropriação indevida de ativos, reportes financeiros fraudulentos ou esquemas Ponzi usados para fraudar os investidores. No entanto, o risco de fraude pode ser reduzido por meio de uma combinação de medidas de prevenção, detecção e dissuasão. A maioria dos esquemas de fraude pode ser evitado com controles internos básicos e auditorias e supervisão eficazes. Infelizmente, a fraude pode ser difícil de detectar porque envolve, frequentemente, o encobrimento por meio de falsificações de documentos, ou o conluio entre membros da gerência, funcionários ou terceiros.

A. Razões para a Fraude

A maior parte das fraudes começam pequenas e continuam crescendo conforme o esquema não é detectado. Por exemplo, os feitores normalmente veem os primeiros roubos como empréstimos temporários que serão devolvidos antes que alguém perceba o problema. O empréstimo vai se tornando mais frequente e os feitores tomam posições indefensáveis ou desenvolvem um esquema para o encobrimento, evitando sua descoberta. Como a fraude continua crescendo, espera-se que ela seja descoberta por um colega de trabalho, pela gerência ou por um auditor interno ou externo.

Os feitores inicialmente exploram os controles internos inadequados para ganho próprio, resultando em danos substanciais à organização. O fraudador típico é do sexo masculino, de meia idade, empregado pela organização já há alguns anos. Ele normalmente trabalha no departamento financeiro e tipicamente comete essas ações em seus próprios termos, motivado pelo dinheiro e pela oportunidade. Muitos estudos indicam que a maioria das fraudes são cometidas por membros da gerência. Os gerentes geralmente têm acesso a informações confidenciais, o que os permite se sobrepor aos controles internos e

infligir danos maiores à organização do que funcionários de menor escalão. Os fraudadores tendem a estar em posições de confiança, a ser educados, pais de família e membros de organizações da comunidade, motivados por uma necessidade pessoal e capazes de racionalizar suas atitudes.

Sem minimizar as circunstâncias individuais de cada esquema de fraude, são as seguintes três características comuns de fraudes:

- A pressão ou incentivo representa uma necessidade que um indivíduo tenta satisfazer, cometendo a fraude. Frequentemente, a pressão vem de uma necessidade financeira ou problema significante. Isso pode incluir a necessidade de manter seu emprego ou ganhar um bônus. Em empresas de capital aberto, pode haver a pressão de atingir ou ultrapassar as estimativas dos analistas. Por exemplo, um grande bônus ou outro prêmio em dinheiro pode ser ganho com base em atingir certas metas de desempenho. O fraudador tem o desejo de manter sua posição na empresa e de também manter um certo padrão de vida, para competir com outros percebidos como estando nesse mesmo nível.

- Oportunidade é a habilidade de cometer fraude e não ser detectado. Como fraudadores não querem ser pegos no ato, eles precisam acreditar que suas atividades não serão detectadas. A oportunidade é criada por controles internos fracos, má gestão, falta de supervisão do conselho e/ou por meio do uso de sua posição e autoridade para se sobrepor aos controles. Não estabelecer os procedimentos adequados para detectar atividades fraudulentas também aumenta as oportunidades de ocorrência da fraude. Um processo pode ser desenvolvido propriamente para condições típicas, mas pode surgir uma oportunidade que crie as circunstâncias necessárias para o controle falhar. Pessoas em posições de autoridade podem ser capazes de criar oportunidades de se sobrepor aos controles existentes, porque seus subordinados ou controles fracos lhes permitem contornar os controles estabelecidos.

    - A oportunidade frequentemente ocorre porque o fraudador sabe o que o auditor fará – o quando, o que e o como dos procedimentos do auditor. Por exemplo, se o fraudador sabe que o auditor sempre testa apenas as transações grandes em dezembro, o fraudador pode cometer fraude em transações menores, em outros meses.

- Racionalização é a habilidade de uma pessoa de justificar uma fraude, um componente crucial na maioria das fraudes. A racionalização envolve uma pessoa, reconciliando seu comportamento (por exemplo, roubo) com as noções comumente aceitas de decência e confiança. Por exemplo, o fraudador se coloca como a prioridade (egocêntrico), em vez de priorizar o bem-estar da organização ou da sociedade como um todo. A pessoa pode acreditar que cometer fraude é justificável no contexto de salvar um membro da família ou algum ente querido, para que possa pagar suas altas despesas médicas. Em outros casos, a pessoa simplesmente categoriza o roubo como "empréstimo" e pretende pagar o dinheiro roubado, posteriormente. Algumas pessoas farão coisas que são definidas como comportamentos inaceitáveis pela organização, mas que são lugares comuns em sua cultura ou que eram aceitas por empregadores anteriores. Como resultado, conseguem racionalizar seu comportamento, como "as regras não se aplicam a eles".

    - A gerência pode reduzir a racionalização por meio de suas

ações, por exemplo, implementando práticas de trabalho e pagamento justo, tratamento imparcial e consistente de funcionários e o *tone at the top* (a gerência modelando o comportamento esperado dos funcionários).

Ter um insight sobre as motivações de um fraudador e reconhecer a ameaça que expõe toda a organização são os primeiros passos para estabelecer e implementar um sistema de gerenciamento de riscos de fraude eficaz e sustentável. Dos três elementos, oportunidade é o que as organizações mais conseguem influenciar. As organizações precisam de procedimentos e controles internos que evitem colocar os funcionários em posições de cometer fraude e que detectem atividades fraudulentas, caso ocorram.

Embora os auditores internos possam não saber o motivo ou racionalização exata que leva à fraude, eles precisam identificar as oportunidades de fraude. Os auditores internos também precisam entender os esquemas e cenários de fraude, assim como ter ciência dos sinais que a indicam e como evitá-las.

B. Exemplos de Fraude

A fraude é perpetrada por uma pessoa ciente de que pode resultar em algum benefício não autorizado a ela, à organização ou a outra pessoa, e pode ser perpetrada por pessoas externas ou internas à organização.

Alguns esquemas comuns de fraude incluem:

- Apropriação indevida de ativos envolve roubar dinheiro ou ativos (suprimentos, inventário, equipamento e informações) da organização. Em muitos casos, o perpetrador tenta ocultar o roubo, normalmente ajudando os registros.

- *Skimming* ocorre quando o dinheiro é roubado de uma organização antes de ser registrado nos livros e registros da organização. Por exemplo, um funcionário aceita um pagamento de um cliente, mas não registra a venda.

- A fraude de desembolso ocorre quando uma pessoa faz com que a organização emita um pagamento por bens ou serviços fictícios, faturas inflacionadas ou faturas de compras pessoais. Por exemplo, um funcionário pode criar uma empresa fantasma e, então, cobrar de seu empregador por serviços inexistentes. Outros exemplos incluem requerimentos de serviços de saúde fraudulentos (cobranças de serviços não prestados, cobranças não agrupadas, em vez de agrupadas), solicitação de seguro-desemprego por pessoas que estão trabalhando ou pedidos de pensão ou bolsa social por pessoas já falecidas.

- A fraude de reembolso de despesas acontece quando um funcionário é pago por despesas fictícias ou inflacionadas. Por exemplo, um funcionário emite um relatório de despesas fraudulento, solicitando o reembolso por viagens pessoais, refeições inexistentes, milhas extras, etc.

- A fraude de folha de pagamento ocorre quando o fraudador faz com que a organização emita um pagamento por conta de pedidos falsos de compensação. Por exemplo, um funcionário solicita o pagamento de horas extras não trabalhadas ou um funcionário acrescenta funcionários fantasmas à folha de pagamento e recebe seus contracheques.

- A fraude de demonstração financeira envolve a representação falsa de demonstrações financeiras, geralmente declarando ativos ou receita a mais ou passivos ou despesas a menos. A fraude de demonstração financeira é normalmente cometida por gerentes de organizações, buscando melhorar a aparência econômica da empresa. Os membros da gerência podem se beneficiar diretamente da

fraude com a venda de ações, recebimento de bônus de desempenho, ou usando o relatório falso para acobertar outra fraude.

- A representação falsa de informações envolve o fornecimento de tais informações falsas, normalmente para pessoas externas à organização. Com maior frequência, isso envolve demonstrações financeiras fraudulentas, embora também possa ocorrer a falsificação de informações usada como medidas de desempenho.

- A corrupção é o mau uso do poder confiado a uma pessoa para ganho privado. A corrupção inclui o suborno e outros usos impróprios de poder. A corrupção é geralmente uma fraude *off-book*, o que significa que há poucas evidências de demonstrações financeiras disponíveis para provar que o crime ocorreu. Funcionários corruptos não precisam alterar fraudulentamente as demonstrações financeiras para encobrir seus crimes; eles simplesmente recebem pagamentos em dinheiro, por baixo dos panos. Na maioria dos casos, esses crimes são descobertos por meio de denúncias ou reclamações de terceiros, normalmente através de um canal de denúncias. A corrupção frequentemente envolve a função de compras. Qualquer funcionário autorizado a gastar o dinheiro da organização é um candidato em potencial à corrupção.

- Suborno é oferecer, dar, receber ou pedir qualquer coisa de valor para influenciar um resultado. Subornos podem ser oferecidos a funcionários chave ou gerentes, como agentes de compras que têm a liberdade de concessão de negócios a fornecedores. Em um caso típico, um agente de compras aceita propina para favorecer um fornecedor externo para a compra de bens ou serviços. O outro lado de oferecer ou receber qualquer coisa de valor é exigi-lo como condição para a concessão de negócios, considerado extorsão econômica. Outro exemplo é um funcionário corrupto de concessão de crédito, exigindo uma propina em troca da aprovação de um empréstimo. Aqueles que pagam as propinas tendem a ser vendedores comissionados ou intermediários para fornecedores externos.

- Um conflito de interesse ocorre quando um funcionário, gerente ou executivo de uma organização tem um interesse pessoal oculto em uma transação que afeta adversamente os interesses da organização, ou dos acionistas.

- Um desvio é o ato de desviar para um funcionário ou pessoa externa à empresa uma transação potencialmente lucrativa que normalmente geraria lucro para a organização.

- O uso não autorizado ou ilegal ou o roubo de informações confidenciais ou registradas para beneficiar erroneamente um indivíduo.

- Atividade de partes relacionadas é uma situação em que uma parte recebe algum benefício não obtenível em uma transação normal, em plena concorrência.

- A sonegação de impostos é o reporte intencional de informações falsas, em uma declaração de imposto de renda, para reduzir os impostos a pagar.

C. Indicadores de Fraudes em Potencial

Fraudadores normalmente exibem certos comportamentos ou características que podem servir como sinais de alerta ou *red flags*. Por exemplo, alguns perpetradores parecem excepcionalmente irritados, alguns de repente começam a gastar excessivamente e outros se tornam cada vez mais reservados em relação a suas atividades. No entanto, a presença desses sintomas não significa em si que

esteja ocorrendo uma fraude ou que ocorrerá no futuro.

Red flags podem ter relação a tempo, frequência, local, quantidade e personalidade. *Red flags* incluem sobreposição de controles pela gerência ou executivos, atividades de gestão irregulares ou mal explicadas, ultrapassar consistentemente as metas/objetivos independentemente da mudança das condições de negócios e/ou concorrência, preponderância de transações ou lançamentos em diário não rotineiros, problemas ou atrasos em fornecer informações solicitadas e mudanças significantes ou incomuns nos clientes ou fornecedores. Os sinais de alerta também incluem transações sem a documentação necessária ou aprovação normal, funcionários ou gerentes entregando cheques em mãos, reclamações de clientes acerca das entregas e controles deficientes de acesso de TI, tais como controles deficientes de senhas.

Red flags pessoais incluem morar melhor do que se pode; mostrar insatisfação com o emprego para colegas de trabalho; associação excepcionalmente próxima com fornecedores; severas perdas financeiras pessoais; vício em drogas, álcool ou apostas; mudanças em circunstâncias pessoais e desenvolver interesses externos de negócios. Além disso, há fraudadores que racionalizam consistentemente o mau desempenho, consideram um desafio intelectual "ganhar do sistema", fornecem comunicações e relatórios não confiáveis e raramente tiram férias ou licenças médicas (e quando estão ausentes, ninguém executa seu trabalho).

Esses sinais de alerta são frequentemente indicadores de má conduta e a gerência e os auditores internos de uma organização precisam estar treinados para entender e identificar os sinais de alerta potenciais de conduta fraudulenta. Embora nada disso signifique que um funcionário esteja, de fato, cometendo fraude, uma combinação desses fatores poderia indicar uma necessidade de investigação e uma crescente atenção da auditoria.

A conscientização contra esquemas de fraude é desenvolvida por meio de avaliações periódicas por parte da gerência ou dos auditores internos, pelo treinamento dos funcionários e pela comunicação frequente entre a gerência e os funcionários.

Papéis/Responsabilidades Típicas para a Prevenção/ Detecção de Fraudes

Uma função de supervisão é importante para prevenir ou dissuadir com eficácia a fraude. A supervisão pode ter diversas formas e pode ser conduzida por muitos, dentro ou fora da organização, sob a supervisão geral do conselho de administração.

Conselho de Administração

O conselho de administração tem responsabilidade sobre a governança eficaz e responsável de fraude corporativa. O papel do conselho é de supervisionar e monitorar as ações da gerência para gerenciar os riscos de fraude. Especificamente, o conselho avalia a identificação dos riscos de fraude, a implementação de medidas antifraude e a criação do *tone at the top,* por parte da gerência. Como o conselho é a autoridade maior de uma organização, ele é responsável por determinar o tom para o gerenciamento do risco de fraude dentro da organização. O conselho pode implementar políticas que encorajem o comportamento ético, incluindo processos para funcionários, clientes e parceiros de relacionamento externo de negócios (EBR – *external business relationships*), para reportar casos nos quais essas políticas tenham sido violadas. O conselho pode monitorar a eficácia do gerenciamento do risco de fraude da organização, indicando um membro da gerência de nível executivo para ser responsável por coordenar o gerenciamento do risco de fraude e reportar ao conselho. Para estabelecer o tom apropriado no topo, o conselho de administração precisa da governança apropriada. Isso engloba todos os aspectos de governança do conselho, incluindo membros do conselho independentes que tenham controle sobre informações e pautas do conselho, acesso à gerência ou conselheiros externos e que cumpram independentemente com as responsabilidades dos comitês de nomeação/ governança, compensação, auditoria e outros comitês.

Comitê de Auditoria

Um comitê de auditoria do conselho de administração atua como os olhos e ouvidos dos investidores e outras partes interessadas. O papel do comitê é avaliar a identificação dos riscos de fraude e a implementação de medidas antifraude por parte da gerência, além de determinar o *tone at the top* de que fraudes não serão aceitas de forma alguma.

O comitê de auditoria normalmente supervisiona a atividade de auditoria interna. A Norma 2060 do IIA: Reporte ao Conselho e à Alta Administração declara que "o DEA deve reportar periodicamente à alta administração e ao conselho sobre o propósito, a autoridade e a responsabilidade da atividade de auditoria interna e o desempenho em relação ao seu planejamento. Os reportes devem também conter a exposição de pontos de riscos significativos e de controles, incluindo os riscos de fraude, os assuntos de governança e outros assuntos necessários ou solicitados pela alta administração e pelo conselho".

O comitê de auditoria é responsável por supervisionar os controles para prevenir ou detectar fraudes na gestão. Neste papel, o comitê de auditoria é responsável por supervisionar a conformidade da alta administração com o reporte financeiro apropriado e por prevenir a sobreposição aos controles por parte da alta administração ou outra influência inapropriada sobre o processo de reporte.

Gerência

A gerência é responsável por supervisionar as atividades dos funcionários e normalmente faz isso por meio da implementação e do monitoramento de processos e controles internos. Além disso, a gerência avalia a vulnerabilidade da entidade a atividades fraudulentas. Fraudes podem ocorrer em qualquer organização, mas o grau e os detalhes envolvidos na avaliação de riscos pode corresponder ao tamanho e à complexidade da organização.

A gerência é responsável por estabelecer e manter um sistema de controle interno eficaz a custos razoáveis. Além disso, as discussões da gerência com investigadores e conselheiros legais desempenham um papel importante no desenvolvimento de controles para o processo de investigação, incluindo o desenvolvimento de políticas e procedimentos para investigações eficazes de fraude e para lidar com os resultados de investigações, reporte e comunicação.

Conselheiro Legal

Os papéis e responsabilidades do conselheiro in-*house* serão guiadas frequentemente pelas leis de cada jurisdição. Um advogado normalmente atua em favor dos interesses da organização e também deve respeitar a confidencialidade do cliente. A descoberta de fraude pode colocar esses dois deveres éticos em um conflito em potencial. Quando em uma situação em que os constituintes de uma organização pretendem se envolver em uma fraude, um advogado, por insistir que reconsiderem sua posição, aconselhá-los a buscar outras opiniões legais ou encaminhar o assunto à autoridade maior da organização. O conselheiro *in-house* pode decidir pedir demissão ao saber de fraudes em potencial ou contínuas, principalmente se o produto do trabalho do conselheiro for usado para levar a fraude adiante. Se o conselheiro se demitir, o conselho geral ou conselho externo pode documentar as medidas tomadas para notificar os membros fraudadores da organização acerca da ilegalidade 1) de sua conduta intencionada ou contínua, 2) das consequências desta conduta e 3) da tentativa do conselheiro de dissuadir a conduta.

Auditores Internos

Os auditores internos avaliam riscos enfrentados por suas organizações, com base em planos de auditoria com testes apropriados. Os auditores internos precisam estar alertas aos sinais e possibilidades de fraude dentro da organização. Enquanto auditores direcionam seu foco a declarações enganosas nas demonstrações financeiras que são materiais, os auditores internos frequentemente se encontram em uma melhor posição para detectar os sintomas que acompanham fraudes. Os auditores internos normalmente têm uma presença constante na organização, o que possibilita um melhor entendimento da organização e de seus sistemas de controle. Especificamente, os auditores internos podem auxiliar na dissuasão da fraude, examinando e avaliando a adequação e a eficácia dos controles internos. Além disso, podem auxiliar a gerência no estabelecimento de medidas eficazes de prevenção de fraudes, já que conhecem as forças e fraquezas da organização e podem fornecer consultoria especializada.

A importância que uma organização atribui à sua atividade de auditoria interna é um indicador do comprometimento da organização com a eficácia do controle interno e do gerenciamento de riscos. Os papéis do auditor interno, em relação ao gerenciamento do risco de fraude, poderiam incluir investigações iniciais ou completas de suspeitas de fraude, análise de causa-raiz e recomendações de melhorias dos controles, monitoramento de um canal de reporte/denúncia e a condução de sessões de treinamento de ética. Se encarregada de tais tarefas, a auditoria interna tem a responsabilidade de obter habilidades e competências suficientes, incluindo conhecimentos sobre esquemas de fraude, técnicas de investigação e leis.

Os auditores internos podem conduzir a auditoria proativa para procurar por apropriações indevidas de ativos e declarações falsas de informações. Isso pode incluir o uso de técnicas de auditoria com auxílio de sistemas, incluindo mineração de dados, para detectar tipos específicos de fraude. Os auditores internos também podem empregar procedimentos analíticos e outros para encontrar itens incomuns e conduzir análises detalhadas de contas e transações de alto risco para identificar fraudes em potencial.

No momento adequado, quando informações suficientes tiverem sido coletadas, o DEA deve manter a alta administração e o comitê de auditoria informados acerca das investigações especiais em progresso e concluídas.

Auditores Externos

Os auditores externos de uma organização têm a responsabilidade de conformidade com as normas profissionais e de planejar e conduzir a auditoria das demonstrações financeiras da organização, para chegarem a uma avaliação razoável de se as demonstrações financeiras estão livres de declarações falsas e se as declarações falsas foram causadas por erro ou fraude. Sempre que um auditor externo tiver determinado que há evidências de que possa haver uma fraude, as normas profissionais do auditor externo tipicamente exigem que o assunto seja encaminhado ao nível apropriado da gerência. O auditor externo normalmente reporta fraudes envolvendo a alta administração diretamente àqueles encarregados da governança (ex.: o comitê de auditoria).

Gerente de Prevenção de Perdas

O gerente de (*loss prevention* – LP) prevenção de perdas (ou grupo de segurança da companhia) lida com as áreas de riscos de negócios como crimes, desastres, acidentes e lixo, que têm a capacidade de levar um negócio à falência. Como *expert* em segurança da organização, o gerente de prevenção de perdas está em uma posição vantajosa para liderar a comunicação de riscos entre outros gerentes de riscos e linha. Ao identificar e entender padrões reais e em potencial dentro do negócio, o gerente de LP pode fornecer *insights* valiosos à gerência acerca da avaliação da eficácia dos processos de gerenciamento de riscos da organização. O gerente de LP normalmente trabalha junto com os auditores internos para identificar áreas de controles internos fracos dentro da organização.

Investigadores de Fraude

Investigadores de fraude são normalmente responsáveis pela detecção e investigação de fraudes, além da recuperação de ativos. Eles também desempenham um papel na prevenção da fraude. A alta administração e o comitê de auditoria precisam apoiar os investigadores para deixar todas as partes interessadas cientes de que a organização está pronta para responder rápida e apropriadamente a riscos de fraude. O alinhamento organizacional da unidade de investigação de fraude (*fraud investigation unit* – FIU) pode variar. Se uma FIU estiver instalada dentro de um departamento de segurança corporativa, pode ser benéfico para eles trabalhar em conjunto ou estar envolvidos nas atividades de auditoria interna, para que os funcionários da FIU tenham acesso às descobertas de auditores internos e independentes. Os investigadores de fraude frequentemente trabalham com o conselheiro legal para tomar medidas legais contra o perpetrador. As comunicações entre os investigadores de fraude e o conselheiro legal, provavelmente serão consideradas confidenciais (ex.: privilegiadas) para permitir um diálogo livre e aberto. Além disso, o trabalho de um investigador de fraude feito sob a direção do conselheiro legal pode ser considerado produto de trabalho protegido de advogado.

O investigador principal normalmente determina o conhecimento, habilidades e outras competências necessárias para conduzir a investigação com eficácia e designa as pessoas competentes e apropriadas para a equipe. Este processo pode incluir a avaliação de que não haja conflito de interesse em potencial com aqueles sendo investigados ou quaisquer outros funcionários da organização.

Outros funcionários

Todo funcionário tem um papel a desempenhar no combate à fraude. Os funcionários são os olhos e os ouvidos da empresa e devem ter a capacidade de manter um ambiente de trabalho íntegro. Os funcionários podem reportar suspeitas de fraude ao canal de denúncias, ao departamento de auditoria interna ou a um membro da gerência. Para dissuadir ou detectar fraude e abuso, muitos especialistas acreditam que um canal de denúncias monitorado apropriadamente é a medida de detecção e dissuasão de fraude de maior custo-benefício.

Responsabilidades de Auditoria Interna durante o Trabalho de Auditoria Interna

Até o ponto em que a fraude possa estar presente em atividades cobertas pelo curso normal do trabalho de auditoria, as *Normas* declaram que os auditores internos têm as seguintes responsabilidades, com respeito à detecção de fraudes:

- Zelo Profissional Devido (Norma 1220)
- Gerenciamento de Riscos (Norma 2120)
- Objetivos do Trabalho de Auditoria (Norma 2210)

No entanto, não se espera que a maioria dos auditores internos tenham o conhecimento equivalente ao daquela pessoa cuja responsabilidade primária seja detectar e investigar fraudes. Além disso, os procedimentos de auditoria, mesmo quando conduzidos com zelo profissional devido, já não garantem que a fraude venha a ser detectada.

Um sistema de controle interno bem desenvolvido deve ajudar a prevenir ou detectar fraudes materiais. Testes conduzidos por auditores internos melhoram a probabilidade de que indicadores importantes de fraude sejam detectados e considerados para mais testes.

A. Conduzindo Trabalhos de Auditoria

Ao conduzir trabalhos de auditoria, o auditor interno deve:

- Considerar riscos de fraude na avaliação do desenvolvimento do controle interno e na determinação dos passos de auditoria a conduzir. Não se espera que os auditores internos detectem fraudes, mas se espera que os auditores internos obtenham uma avaliação razoável de que os objetivos do negócio para o processo sob revisão estão sendo atingidos e de que deficiências de controle – seja por simples erro ou esforço intencional – estão sendo detectadas. A consideração de riscos de fraude é documentada nos papéis de trabalho, assim como a ligação dos riscos de fraude ao trabalho de auditoria específico.
- Ter conhecimento suficiente de fraudes para identificar *red flags*, indicando que fraudes foram cometidas. Este conhecimento inclui as características da fraude, as técnicas usadas para cometer fraudes e os diversos esquemas e cenários de fraude associados às atividades sob revisão.
- Estar alerta a oportunidades que poderiam possibilitar fraudes, como deficiências de controle. Se deficiências significantes de controle forem detectadas, testes adicionais conduzidos por auditores internos podem ser usados para identificar se foi cometida uma fraude.
- Avaliar se a gerência está cumprindo ativamente com sua responsabilidade de supervisão do programa de gerenciamento do risco de fraude, se medidas corretivas oportunas e suficientes foram tomadas com relação a quaisquer deficiências ou fraquezas de controle detectadas e se o plano para monitoramento do programa continua sendo adequado ao sucesso contínuo do programa.
- Avaliar os indicadores de fraude e decidir se alguma outra ação é necessária ou se uma investigação deve ser recomendada.
- Recomendar uma investigação, quando apropriado.

O Anexo B inclui algumas questões que a auditoria interna pode considerar normalmente em suas avaliações de um programa contínuo de gerenciamento do risco de fraude.

B. Ceticismo do Auditor Interno

O ceticismo profissional é uma atitude que inclui uma mentalidade questionadora e uma avaliação crítica de evidências de auditoria. Um auditor interno objetivo e cético não presume que a gerência ou os funcionários sejam desonestos, tampouco presume uma honestidade inquestionável.

Em todo trabalho de auditoria, o exercício do ceticismo profissional é primordial. O ceticismo profissional inadequado é citado frequentemente como um motivo significante pelo qual fraudes materiais não foram detectadas. Os auditores internos desempenham um papel crítico no sucesso ou fracasso do gerenciamento do risco de fraude. Com seu conhecimento íntimo do funcionamento de uma entidade, os auditores internos estão em uma posição única para identificar muitos dos indicadores de fraude. Quando os auditores internos agem com ceticismo e voltam seu foco para a eficácia dos controles internos, a probabilidade de notarem as características comuns de fraude aumenta e podem descobrir possíveis atividades fraudulentas, se e onde existirem.

Para permitir aos auditores internos o exercício do ceticismo, a Norma 1111 do IIA: Interação Direta com o Conselho declara que o DEA deve se comunicar e interagir diretamente com o conselho. Além disso, a Norma 1120: Objetividade Individual declara que os auditores internos devem adotar uma atitude imparcial e isenta e evitar qualquer conflito de interesses, o que é consistente com o exercício do ceticismo. A supervisão e o apoio do comitê de auditoria à atividade de auditoria interna ajuda o auditor interno a manter sua independência e objetividade, assim como a manter uma atitude de ceticismo.

C. Comunicação com o Conselho

A relação entre o DEA e o conselho de administração inclui as funções de reporte e supervisão. Os auditores internos, por meio do papel único que desempenham, estão bem posicionados para elevar a importância dos programas de prevenção e detecção de fraude com a gerência e o conselho. Estar ciente do que está acontecendo em sua indústria e organização especificamente melhorará a habilidade dos auditores internos de abordar os riscos de fraude junto ao conselho.

Em discussões com o conselho, o DEA pode incluir:

- Todas as auditorias de fraude conduzidas.
- O processo de avaliação do risco de fraude.
- Fraudes ou conflitos de interesse e resultados dos programas de monitoramento com relação à conformidade com a lei, código de conduta e/ou ética.
- A estrutura organizacional da atividade de auditoria interna, conforme for necessário para abordar o assunto de fraude.
- A coordenação da atividade de auditoria de fraude com auditores externos.
- A avaliação geral do ambiente de controle da organização.
- Medidas de produtividade e orçamento das atividades de fraude da auditoria interna.
- Comparações com referências (*benchmarking*) das atividades de fraude da auditoria interna com outras organizações.
- O papel da auditoria interna nas investigações de fraude.

O DEA pode ter uma opinião diferente da opinião da alta administração e do conselho, com relação ao momento certo para informá-los de questões sérias, incluindo fraudes. Uma solução para lidar com essa preocupação de *timing* é que o DEA tenha discussões com a alta administração e o conselho, antes que surjam essas questões, para saber de que necessitam estar cientes, quando precisam ser informados e como a comunicação deve ser feita. Conduzir essa discussão é um sinal de que o DEA está em conformidade com a Norma 2060 do IIA: Reporte à Alta Administração e ao Conselho. A ilustração a seguir mostra um exemplo de um documento que pode ser preparado para esclarecer a natureza e *timing* da comunicação do DEA com o conselho, com relação a questões de fraude.

Amostra de Matriz de Eventos do Comitê de Auditoria			Quando os Eventos Devem ser Reportados ao Comitê de Auditoria			
	Evento	Magnitude	Imediatamente	Na próxima reunião	Relatório Anual	Resumo Anual
1	Desfalque, fraude, roubo:					
	Não envolvendo a alta administração					
	Grande quebra nos controles	Mais do que $10.000	X			
	Envolve encobrimento	Mais do que $10.000		X		
	Pequeno	Menos do que $10.000				X
	Envolvendo a alta administração	Todos	X			
2	Recusa de acesso da auditoria interna a pessoas ou dados	Todos	X			
3	Violação da Política de Ética					
	Alta administração	Todos	X			
	Gerência média	Todos		X		
4	Discussão sobre a substituição do DEA	Todas as atividades com antecedência	X			

Avaliação do Risco de Fraude

Todas as organizações estão expostas ao risco de fraude em qualquer processo em que seja necessário o envolvimento humano. A exposição de uma organização à fraude é uma função dos riscos de fraude inerentes ao negócio, o ponto até o qual haja controles internos eficazes para prevenir ou detectar fraudes e a honestidade e a integridade daqueles envolvidos no processo.

O risco de fraude é a probabilidade de que uma fraude vá ocorrer e as consequências em potencial para a organização, quando isso ocorrer. A probabilidade de uma atividade fraudulenta é baseada, tipicamente, no grau de facilidade de cometer fraude, nos fatores motivacionais que levam à fraude e no histórico de fraude da organização.

Uma avaliação do risco de fraude é normalmente um componente crítico do maior programa de gerenciamento de riscos corporativos de uma organização. A avaliação do risco de fraude é uma ferramenta que auxilia a gerência e os auditores internos a identificar sistematicamente onde e como uma fraude pode ocorrer e quem pode estar em uma posição de cometê-la. Uma revisão de exposições em potencial representa um passo inicial para tratar das preocupações do conselho e da alta administração com os riscos de fraude e de sua habilidade de alcançar as metas organizacionais, enquanto promovem a confiança pública na saúde de uma organização. Uma avaliação do risco de fraude é centrada em esquemas e cenários de fraude, para determinar a presença de controles internos e se os controles podem ser contornados.

Um papel importante da gerência é o de supervisionar a conclusão bem sucedida de uma avaliação do risco de fraude, de modo que a gerência tenha um entendimento melhor dos riscos de fraude e dos controles em prática para mitigar estes riscos. As organizações precisarão chegar a suas próprias conclusões com relação ao custo de controlar um risco, em comparação com os benefícios de mitigar e eliminar este risco.

Uma avaliação do risco de fraude geralmente inclui cinco passos principais:

1. Identificar fatores relevantes do risco de fraude.
2. Identificar esquemas de fraude em potencial e priorizá-los com base em riscos.
3. Mapear os controles existentes para esquemas de fraude em potencial e identificar lacunas.
4. Testar a eficácia operacional dos controles de prevenção e detecção de fraudes.
5. Documentar e reportar a avaliação do risco de fraude.

O escopo da avaliação do risco de fraude pode variar amplamente, dependendo do tamanho, complexidade ou indústria da organização. Por exemplo, um negócio online que tem poucos funcionários, com inventário limitado e pouco dinheiro em espécie teria provavelmente riscos de fraude diferentes dos riscos de uma organização com inúmeros locais físicos e uma grande base de funcionários com acesso ao inventário e/ou dinheiro. Uma organização pode completar uma avaliação de toda a empresa e incluir todas as áreas de negócios na avaliação, enquanto a outra organização pode limitar seu foco à área de risco de negócios mais importantes. Uma organização com muitas subsidiárias pode completar uma avaliação separada para cada subsidiária ou uma avaliação combinada.

A. Identificando Fatores Relevantes do Risco de Fraude

O primeiro passo é coletar informações sobre as atividades de negócios da organização, para ter um entendimento dos riscos de fraude, incluindo os parceiros de relações externas de negócios. Este processo abrange a revisão da documentação de fraudes anteriores e de suspeitas de fraudes

cometidas contra ou em prol da organização, a avaliação das fraudes relacionadas em organizações similares e a revisão das medidas de desempenho da organização nos últimos anos, em comparação com empresas concorrentes. Por exemplo, padrões inconsistentes entre medidas não financeiras e financeiras, uso excessivo de software licenciado e o uso de propriedades intelectuais de outra pessoa podem indicar uma possível fraude.

B. Identificando e Priorizando Esquemas de Fraude em Potencial com Base em Riscos

A *fraude*, por definição, significa uma má conduta intencional com o objetivo de evitar detecção. Como tal, uma equipe de avaliação do risco de fraude precisa ter um raciocínio estratégico para antecipar tanto o esquema de fraude quanto os indivíduos dentro ou fora da organização que poderiam estar em uma posição de perpetrar cada esquema. Uma equipe de avaliação do risco de fraude é composta, tipicamente, de indivíduos da atividade de auditoria interna, finanças, jurídico, TI, segurança e potencialmente outras funções, dependendo da natureza da organização.

A equipe de avaliação do risco de fraude identifica esquemas de fraude em potencial, usando *brainstorming*, entrevistas com a gerência, procedimentos analíticos e revisões de fraudes anteriores. Durante este processo, a equipe de avaliação do risco de fraude examina as atividades, esquemas relevantes à indústria, geografia e programas da organização, sempre considerando as características básicas da fraude (pressão/incentivo, oportunidade e racionalização), questionando:

- Onde estão as oportunidades para fraude?
- Qual o nível de pressão sob o qual a gerência se encontra, que a levaria à sobreposição dos controles internos?
- Há alguma consequência se a gerência não alcançar as metas?

Áreas específicas de fraude devem ser identificadas sem considerar os controles internos existentes ou eficazes (o que será feito posteriormente). A avaliação considera se a fraude poderia ser cometida por um indivíduo apenas ou se requer conluio entre funcionários ou pessoas externas à organização.

Os seguintes fatores são considerados na priorização dos riscos de fraude:

- Impacto monetário
- Impacto à reputação da organização
- Perda de produtividade
- Ações criminais/civis em potencial, incluindo não conformidade regulatória
- Integridade e segurança dos dados
- Perda de ativos
- Localização e porte das operações/unidades
- Cultura da companhia
- Rotatividade da gerência/funcionários
- Liquidez dos ativos
- Volume e/ou tamanho das transações
- Terceirização

C. Mapeando os Controles Existentes para Esquemas de Fraude em Potencial e Identificando Lacunas

A equipe de avaliação do risco de fraude identifica os controles preventivos e de detecção em prática para lidar com cada risco de fraude e para avaliar a probabilidade e importância de cada fraude em potencial. Controles corporativos antifraude, tais como a existência de um canal de denúncias anônimas e uma política de proteção ao denunciante, supervisão do conselho, resultados do

monitoramento contínuo, código de conduta e o tom das comunicações da gerência com relação à sua tolerância ao risco de fraude são elementos importantes neste exercício. O risco da sobreposição da gerência aos controles precisa ser considerado explicitamente e o custo-benefício do controle deste risco deve ser avaliado.

D. Testando a Eficácia Operacional dos Controles de Prevenção e Detecção de Fraudes

A auditoria interna desempenha um papel tipicamente importante na avaliação da eficácia operacional dos controles internos. Os auditores internos não consideram apenas a existência do controle interno, mas também a eficácia deste controle interno, ao longo de testes periódicos do referido controle. Por exemplo, uma organização pode implementar uma política de segurança para as senhas da rede, exigindo que as senhas sejam alteradas a cada 30 dias; no entanto, os controles de acesso ao sistema da rede não bloqueiam o acesso do usuário se a senha não for modificada como exigido. Neste caso, o controle interno existe, mas não é operacionalmente eficaz.

E. Documentando e Reportando a Avaliação do Risco de Fraude

As organizações precisam documentar o processo que identifica e avalia o risco de fraude. Os elementos-chave que seriam provavelmente documentados em uma avaliação do risco de fraude para cada área significante de negócios incluem:

- Os tipos de fraude que têm alguma chance de ocorrer.
- O risco inerente de fraude, considerando a disponibilidade de ativos líquidos e vendíveis, moral organizacional e rotatividade dos funcionários, o histórico de fraudes e perdas e outros indicadores da área de negócios específica.
- A adequação de programas antifraude existentes, monitoramento e controles de prevenção.
- As lacunas potenciais nos controles de fraude da organização, incluindo a segregação de funções.
- A probabilidade de ocorrer uma fraude significante.
- O impacto/importância de uma fraude para o negócio.

De acordo com a Norma 2060 do IIA: Reporte à Alta Administração e ao Conselho, o DEA deve reportar periodicamente à alta administração e ao conselho exposições significantes a riscos e questões de controle, incluindo riscos de fraude. A gerência e o DEA mantêm o conselho informado periodicamente sobre o status e resultados da avaliação do risco de fraude. Estas atualizações reportam sobre a eficácia dos programas antifraude existentes, assim como dos esforços corretivos feitos pela gerência para lidar com as lacunas identificadas durante a avaliação.

Consulte o Anexo C para ver um exemplo de avaliação do risco de fraude. Este modelo pode ser adaptado para uma avaliação do risco de fraude de toda a organização, incluindo as principais áreas/unidades de negócios na estrutura.

Prevenção e Detecção de Fraude

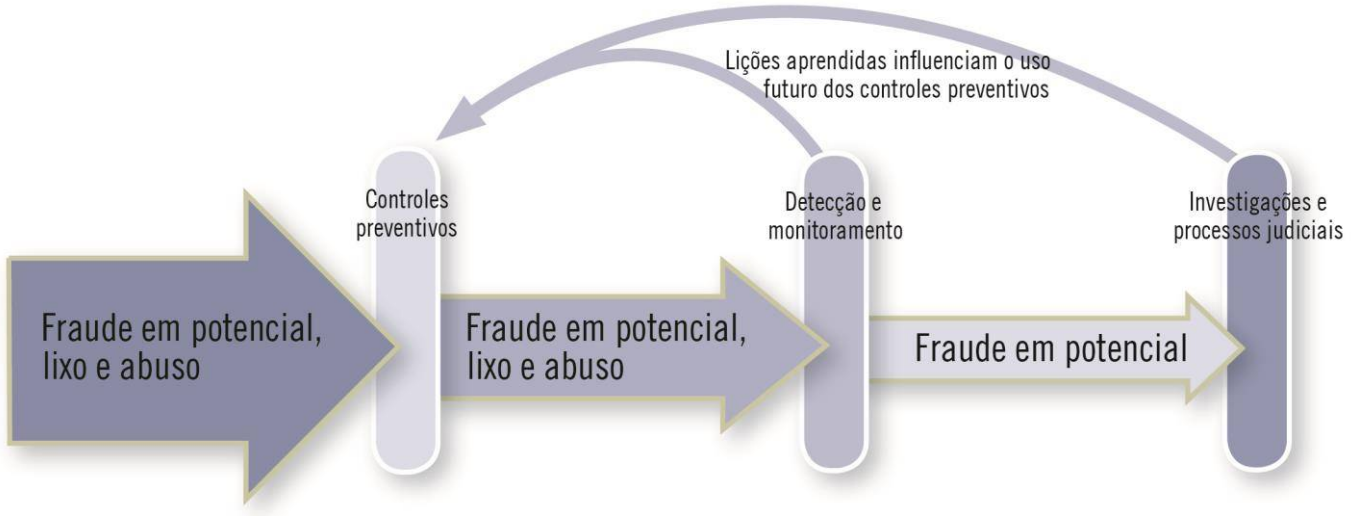
A fraude pode ocorrer em diversos níveis da organização; portanto, é importante estabelecer técnicas apropriadas de prevenção e detecção. Embora a prevenção e a detecção de fraudes sejam conceitos relacionados, eles não são a mesma coisa. A prevenção de fraudes significa a implementação de políticas e procedimentos, treinamento de funcionários e a comunicação da gerência para educar os funcionários acerca de atividades fraudulentas. Por outro lado, a detecção de fraudes engloba as atividades e programas desenvolvidos para identificar fraude ou má conduta que esteja ocorrendo ou tenha ocorrido. A interrelação entre prevenção, detecção e investigação de fraudes é ilustrada no gráfico abaixo.

As organizações nunca podem eliminar o risco de fraude. Há sempre pessoas motivadas a cometer fraude e pode surgir uma oportunidade de alguém na organização se sobrepôr aos controles internos ou entrar em conluio com outros para driblar os controles internos. Embora toda organização seja suscetível à fraude, não é rentável tentar eliminar todo o risco de fraude. Uma organização pode escolher desenvolver seus controles para detectar, em vez de prevenir os riscos de fraude. Se o custo do desenvolvimento, implementação e monitoramento dos controles internos contra a fraude exceder o impacto estimado do risco, pode não ser rentável implementar os controles internos.

Para entender e avaliar a oportunidade de ocorrência de fraude na organização é preciso compreender a cultura corporativa. A cultura corporativa traz uma visão holística e abrangente da filosofia geral de gestão e do ambiente de controle. Apenas uma cultura corporativa ética forte não protege a organização da fraude. Embora cultivar uma cultura ética seja um primeiro passo essencial, reduzir o risco de fraude também exige treinamento e educação, políticas e procedimentos fortes para implementar e monitorar os controles internos, procedimentos para detectar indicadores do risco de fraude de forma oportuna para investigar fraudes e, quando apropriado, para levar o caso à Justiça.

A. Prevenção da Fraude

A prevenção da fraude envolve as ações tomadas para desencorajar a fraude e limitar a exposição à mesma, quando ela ocorrer. Instilar uma cultura ética forte e estabelecer o tom correto no topo são elementos essenciais para a prevenção da fraude. Um mecanismo principal forte para a prevenção da fraude são controles internos eficazes e eficientes, incluindo controles relativos a filtrar consumidores, fornecedores e parceiros de relações de negócios externos. Uma organização com controles internos eficazes dissuade os fraudadores da tentação de cometer fraude. A gerência é a principal responsável



por estabelecer e manter os controles internos em uma organização. O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) apresentou uma estrutura para avaliar e melhorar os sistemas de controles internos para combater a fraude. O COSO identificou cinco componentes em sua *Estrutura Integrada - Controle Interno*: o ambiente de controle, a avaliação de riscos, as atividades de controle, informação e comunicação, e o monitoramento, que podem servir como premissa para o desenvolvimento de controles para combate à fraude. Os elementos são profundamente ligados e sobrepostos em sua natureza e fornecem um processo interativo natural para promover o tipo de ambiente no qual a fraude não será tolerada, em nível algum.

Ambiente de controle – Os elementos de um ambiente de controle forte ajudam a prevenir a fraude, incluindo os seguintes:

- Um código de conduta, política de ética ou política de fraude, para estabelecer o *tone at the top* apropriado.
- Programas de ética e de denúncias anônimas para reportar preocupações.
- Diretrizes e práticas de contratação e promoção .
- Supervisão por parte do comitê de auditoria, conselho ou outros órgãos supervisores.

Avaliação de Risco – Estabelecimento de um processo de avaliação do risco de fraude que considere os fatores do risco de fraude e seus esquemas.

- Envolver o pessoal apropriado no processo de avaliação do risco de fraude.
- Conduzir avaliações do risco de fraude, regularmente.

Atividades de controle – Políticas e procedimentos para processos de negócios, incluindo limites apropriados de autoridade e segregação de funções incompatíveis.

Informação e comunicação – Promoção da importância do programa de gerenciamento do risco de fraude e da posição da organização acerca do risco de fraude, tanto interna quando externamente, por meio de programas de comunicação corporativa.

- Desenvolvimento e entrega de treinamentos de conscientização contra a fraude.
- Um processo de afirmação ou certificação para confirmar que os funcionários leram e entenderam as políticas corporativas e que os funcionários estão em conformidade com as políticas.

Monitoramento – Fornecimento de avaliações periódicas dos controles antifraude.

- Usando avaliações independentes do programa de gerenciamento do risco de fraude, por parte da auditoria interna ou outros grupos.
- Implementando tecnologias para auxiliar nas atividades contínuas de monitoramento e detecção.

B. Treinamento de Prevenção da Fraude

O treinamento de prevenção da fraude é normalmente um fator chave na deterrência da fraude. O treinamento pode cobrir as expectativas da organização com relação à conduta dos funcionários, os procedimentos e normas necessárias para implementar os controles internos, os papéis e responsabilidades dos funcionários de reporte de má conduta. Os funcionários precisam entender o comportamento ético que deles é esperado para agir de acordo, dentro da organização. Orientações a novos funcionários podem apresentar a missão, os valores e o código de conduta da organização, tipos de fraudes, responsabilidade de reporte de violações de comportamento ético e impropriedade, detalhes

do canal de denúncias e outros meios de reportar fraudes em potencial.

O treinamento de funcionários contra a fraude precisa ser feito sob medida para a organização e a posição do funcionário dentro da empresa. Embora treinamentos genéricos de prevenção da fraude possam ser úteis, é mais eficaz identificar as principais áreas de risco de fraude na organização e desenvolver um treinamento que permita que os funcionários, em posições-chave, entendam seu papel no programa de detecção de fraude da organização. Os fraudadores podem até participar do treinamento, o que pode beneficiar a organização, já que podem ser dissuadidos ao verem o processo de gerenciamento do risco de fraude da organização em ação.

O treinamento periódico ao longo da carreira do funcionário reforça a conscientização contra a fraude e o custo da fraude para a organização. Independentemente do método usado para produzir e disseminar o material de treinamento, uma meta principal é tentar a compreensão do funcionário acerca do treinamento contra fraude. Isso pode ser feito por meio de pesquisas online que não apenas confirmem a presença do funcionário, mas que também ofereçam testes rápidos para determinar se os funcionários obtiveram o conhecimento necessário, a partir do treinamento.

C. Detecção de Fraude

Controles de detecção são desenvolvidos para fornecer avisos ou evidências de que uma fraude esteja ocorrendo ou tenha ocorrido. Controles internos eficazes são um dos deterrentes mais fortes do comportamento e das ações fraudulentas. O uso simultâneo de controles internos preventivos e detectivos aumenta a eficácia de qualquer programa de gerenciamento do risco de fraude. Embora os controles internos detectivos possam fornecer evidências de fraude, eles não têm o objetivo de preveni-la.

Os métodos de detecção de fraude precisam ser flexíveis, adaptáveis e em constante mudança para acompanhar as mudanças do ambiente de riscos. Embora as medidas preventivas sejam aparentes e rapidamente identificáveis, os controles detectivos podem não ser tão aparentes (isto é, eles operam em segundo plano).

As organizações frequentemente contam com os funcionários para o reporte de atividades suspeitas, por meio de um canal de denúncias anônimas. Usar o feedback dos funcionários permite capitalizar em cima do fato de que muitos deles, dentro da organização, desejam compartilhar o que sabem sobre as questões organizacionais. Uma forma eficaz para a organização ficar sabendo de uma fraude existente é oferecer aos funcionários, fornecedores e outras partes interessadas uma variedade de métodos de reporte de suas preocupações sobre comportamento ilegal ou antiético. Formas de coletar estas informações incluem:

- Confirmação do Código de Conduta – Quando o funcionário assinar o código anual de conduta, que determina suas responsabilidades na prevenção e detecção de fraudes, é possível pedir que reporte qualquer violação de que ele tenha ciência.

- Canal de denúncias – Pode ser uma linha telefônica ou um sistema de reporte online, no qual o denunciante possa permanecer anônimo.

- Entrevistas de saída – Conduzir entrevistas de saída com funcionários demitidos ou com aqueles que pediram demissão pode ajudar a identificar esquemas de fraude. Elas também podem ajudar a determinar se há questões relacionadas à integridade da gerência e podem fornecer informações, com relação às condições que levam à fraude.

- Pesquisa proativa para funcionários – pesquisas rotineiras para os funcionários podem ser conduzidas para coletar conhecimentos de fraude ou comportamento antiético, dentro da organização. Uma

> pesquisa proativa poderia provocar a entrega de informações anônimas por parte dos funcionários, o que ajudaria as organizações a detectar fraudes mais cedo do que o fariam se esperassem que os funcionários revelassem a informação, deliberadamente.

Todos estes métodos podem usar entrevistas tradicionais por telefone, formulários online, e-mails, fax e reuniões em pessoa.

Outros métodos de detecção de fraude incluem auditorias surpresas, em áreas de alto risco de fraude por parte da auditoria interna, externa ou da gerência; o monitoramento contínuo de dados críticos e tendências relacionadas para identificar situações incomuns ou variações; e comparações rotineiras e/ou ad-hoc de dados públicos e/ou registrados com transações relevantes, listas de fornecedores, rol de funcionários e outros dados.

Investigação de Fraude

As organizações investigam possíveis fraudes, quando há uma preocupação ou suspeita de transgressões dentro da organização. As suspeitas podem ser resultantes de um processo de reclamação formal, de um processo de reclamação informal, como dicas, ou uma auditoria, incluindo uma auditoria desenvolvida para fazer testes buscando fraudes. Investigar uma fraude não é o mesmo que fazer uma auditoria de fraude, que é uma auditoria desenvolvida para detectar proativamente indicadores de fraude nos processos ou transações em que as análises indiquem que o risco de fraude é significante.

Uma investigação de fraude consiste em coletar informações suficientes sobre detalhes específicos e realizar os procedimentos necessários para determinar se a fraude ocorreu, a perda ou exposição associada à fraude, quem estava envolvido e como aconteceu. Um resultado importante das investigações é que as pessoas inocentes sejam, de fato, inocentadas de suspeitas.

As investigações buscam descobrir a natureza e extensão total da atividade fraudulenta, não apenas o evento que pode ter iniciado a investigação. O trabalho de investigação inclui a preparação, documentação e preservação de evidências suficientes para processos judiciais em potencial.

Auditores internos, advogados, investigadores, pessoal de segurança e outros especialistas internos e externos à organização normalmente conduzem ou participam das investigações de fraude.

As investigações e as atividades de resolução relacionadas precisam ser cuidadosamente gerenciadas de acordo com as leis. A legislação local pode direcionar como e onde as investigações devem ser conduzidas, práticas disciplinares e de recuperação, e comunicações investigativas. É em favor dos interesses da companhia, tanto profissional quanto legalmente, que se trabalhe com eficácia com o conselheiro legal da empresa e que se esteja familiarizado com as leis relevantes no país em que a fraude ocorre.

A. Processo de Investigação

A gerência é responsável pelo desenvolvimento de controles sobre o processo de investigação, incluindo o desenvolvimento de políticas e procedimentos para investigações eficazes, a preservação de evidências, a aplicação dos resultados das investigações, relatórios e comunicações. Tais normas são muitas vezes documentadas em uma política de fraude; auditores internos podem auxiliar na avaliação da política. Tais políticas e procedimentos precisam considerar os direitos dos indivíduos, a qualificação das pessoas autorizadas a conduzir as investigações e as leis relevantes onde ocorreram as fraudes. As políticas devem também considerar até que ponto a gerência vai disciplinar funcionários, fornecedores ou clientes, incluindo a adoção de medidas legais para recuperar as perdas e processos civis ou criminais. É importante que a gerência defina claramente a autoridade e as responsabilidades das pessoas envolvidas na investigação, especialmente a relação entre o investigador e o conselheiro legal. Também é importante que a gerência desenvolva e cumpra com os procedimentos que minimizam a comunicação interna sobre uma investigação em curso, especialmente nas fases iniciais.

A política precisa especificar o papel do investigador em determinar se a fraude foi cometida. O investigador ou a gerência decidirá se houve fraude e a gerência decidirá se a organização irá notificar as autoridades externas. Um julgamento de que a fraude ocorreu pode, em algumas jurisdições, ser feito apenas por autoridades policiais ou judiciais. A investigação pode simplesmente resultar em uma conclusão de que a política da organização foi violada ou de que é provável que a fraude tenha ocorrido.

B. O Papel da Auditoria Interna nas Investigações

O papel da atividade de auditoria interna nas investigações precisa ser definido no estatuto da

auditoria interna, assim como nas políticas e procedimentos contra fraude. Por exemplo, a auditoria interna pode ser a principal responsável pelas investigações de fraude, pode atuar como um recurso para as investigações ou pode se abster de envolvimento nas investigações. A auditoria interna pode se abster de envolvimento, porque é responsável pela avaliação da eficácia das investigações ou porque não tem os recursos apropriados para este envolvimento. Qualquer um desses papéis pode ser aceitável, desde que o impacto dessas atividades da independência da auditoria interna seja reconhecido e abordado apropriadamente.

Para manter a proficiência, as equipes de investigação de fraude têm a responsabilidade de obter conhecimentos suficientes sobre esquemas fraudulentos, técnicas de investigação e leis aplicáveis. Há programas nacionais e internacionais que fornecem treinamento e certificações para investigadores e especialistas forenses.

Se a atividade de auditoria interna for responsável pela investigação, ela pode conduzi-la, usando a equipe *in-house*, terceirizada ou uma combinação de ambas. Em alguns casos, a auditoria interna pode também usar funcionários de fora do departamento de auditoria da organização, para auxiliar. É geralmente importante reunir a equipe de investigação sem delongas. Se a organização provavelmente precisará de especialistas, o DEA pode pré-qualificar o(s) prestador(es) de serviços, para que recursos externos estejam disponíveis rapidamente quando necessários.

Em organizações em que a principal responsável pela função de investigação não é a atividade de auditoria interna, é possível ainda solicitar à auditoria interna que auxilie na coleta de informações e que faça recomendações de melhorias nos controles internos.

C. Conduzindo a Investigação

Um plano de investigação é desenvolvido para cada investigação, seguindo os procedimentos ou protocolos de investigação da empresa. O investigador principal determina o conhecimento, as habilidades e outras competências necessárias para conduzir a investigação com eficácia e designa as pessoas competentes e apropriadas para a equipe. Este processo inclui obter uma avaliação de que não haja conflito de interesses em potencial, com aqueles sendo investigados ou com quaisquer outros funcionários da organização.

O plano deve considerar as seguintes atividades investigativas:

- Coleta de evidências por meio de vigilância, entrevistas ou declarações por escrito.
- Documentação e preservação de evidências, considerando as regras legais de evidência e os usos da evidência do ponto de vista do negócio.
- Determinação da extensão da fraude.
- Determinação das técnicas usadas para cometer a fraude.
- Avaliação da causa da fraude.
- Identificação dos perpetradores.

A qualquer momento durante esse processo, o investigador pode concluir que a reclamação ou suspeita foi infundada e, então, o investigador seguirá o processo da organização para encerrar o caso.

Os procedimentos específicos empregados em cada investigação vão variar com base na situação específica e nas metas da equipe investigativa. Os procedimentos investigativos comuns incluem:

- Obter evidências: A coleta e a preparação de evidências são críticas para o entendimento da fraude ou má conduta e são necessárias para embasar as conclusões da equipe investigativa. A equipe investigativa pode usar procedimentos forenses em computador

ou análise de dados com auxílio de sistemas, com base na natureza das alegações, nos resultados dos procedimentos realizados e nas metas da investigação. Todos os relatórios, documentos e evidências obtidas devem ser registrados cronologicamente em um inventário ou *log*. Alguns exemplos de evidências incluem:

- Cartas, memorandos e correspondências, tanto em cópia impressa quanto em formato eletrônico (como e-mails ou informações armazenadas em computadores pessoais).
- Arquivos de computador, postagens gerais em livro ou outros registros financeiros ou eletrônicos.
- Registros de TI ou de acesso ao sistema.
- *Logs* de monitoramento de horas e de segurança, tais como vídeos de câmeras de segurança ou registros de crachá de acesso.
- Registros telefônicos internos.
- Informações de clientes ou fornecedores, tanto em domínio público quanto mantidas pela organização, tais como contratos, faturas e informações de pagamento.
- Registros públicos, tais como o registro do negócio junto a agências governamentais ou registros de propriedade.
- Artigos de jornal, *websites* internos ou externos, tais como sites de redes sociais.

- Entrevistas: o investigador entrevistará indivíduos, tais como testemunhas e profissionais de facilitação. Tipicamente, o indivíduo acusado é entrevistado depois que a maior parte das evidências aplicáveis já foi obtida. Muitos investigadores preferem abordar o acusado com evidências suficientes para apoiar a meta de garantir uma confissão. Geralmente, o acusado é entrevistado por duas pessoas: 1) um investigador experiente e 2) um outro indivíduo, que toma nota durante a entrevista e, posteriormente, atua como testemunha, se necessário. Além disso, é essencial que todas as informações obtidas na entrevista sejam reportadas corretamente.

As atividades investigativas precisam ser coordenadas com a gerência, o conselheiro legal e outros especialistas, tais como recursos humanos e a gerência de riscos de seguro, conforme for apropriado durante a investigação.

Os investigadores precisam ser versados e conhecedores dos direitos das pessoas dentro do escopo da investigação e da reputação da organização em si. O investigador tem a responsabilidade de garantir que o processo de investigação seja conduzido de forma consistente e prudente.

O nível e a extensão de cumplicidade na fraude em toda a organização precisam ser avaliados. Esta avaliação pode ser crítica para não destruir ou contaminar evidências cruciais e para evitar a obtenção de informações enganosas de pessoas que podem estar envolvidas.

A investigação precisa proteger adequadamente as evidências coletadas, mantendo os procedimentos de cadeia de custódia apropriados à situação.

D. Reportando Investigações de Fraude

O reporte das investigações de fraude consiste de diversas comunicações orais, escritas, interinas ou finais à alta administração e/ou ao conselho, com relação ao status e ao resultado das investigações de fraude. Os relatórios podem ser preliminares e contínuos durante a investigação.

Um relatório escrito ou outra comunicação formal pode ser emitido ao final da fase de investigação. Ele pode incluir a razão da investigação, cronogramas, observações, conclusões, resolução e ações corretivas tomadas (ou recomendações) para melhorar os controles. Dependendo de como a investigação foi resolvida, o relatório pode precisar ser escrito de forma a garantir confidencialidade a algumas das pessoas envolvidas. Ao redigir o relatório, o investigador precisa considerar as necessidades do conselho e da gerência, ao mesmo tempo, mantendo a conformidade com os requisitos e restrições legais e com as políticas e procedimentos da organização.

Considerações adicionais com relação ao reporte de fraude são:

- Enviar um rascunho das comunicações finais propostas sobre fraude ao conselheiro legal para revisão. Em casos em que a organização seja capaz de recorrer ao sigilo advogado-cliente, e tenha escolhido fazê-lo, o relatório é destinado ao conselheiro legal.

- Notificar, de forma oportuna, a alta administração e o conselho, quando houver fraude ou desgaste de confiança significante.

- Os resultados de uma investigação de fraude podem indicar que a fraude teve um efeito adverso, não descoberto, previamente, sobre a posição financeira da organização e sobre seus resultados operacionais de um ou mais anos, para os quais já foram emitidas as demonstrações financeiras. A alta administração e o conselho precisam ser informados desta descoberta, para que possam decidir sobre o reporte apropriado, normalmente depois de consultar os auditores externos.

Se a auditoria interna conduzir a investigação, a Norma 2400 do IIA: Comunicação dos Resultados fornece informações aplicáveis às comunicações necessárias do trabalho.

E. Resolução de Incidentes de Fraude

A resolução consiste em determinar quais ações serão tomadas pela organização, uma vez que o esquema de fraude e o(s) perpetrador(es) tiverem sido plenamente investigados e as evidências tiverem sido examinadas. A gerência e o conselho são responsáveis por resolver incidentes de fraude – e não a atividade de auditoria interna ou o investigador.

A resolução pode incluir todos ou alguns dos itens abaixo:

- Dar conclusão às pessoas que estiveram inicialmente sob suspeita, mas foram inocentadas.

- Dar conclusão àqueles que reportaram a questão.

- Disciplinar um funcionário de acordo com as políticas da organização, legislação do trabalho ou contratos de trabalho.

- Solicitar a restituição financeira voluntária ao funcionário, cliente ou fornecedor.

- Terminar os contratos com fornecedores.

- Reportar o incidente à polícia, órgãos regulatórios ou autoridades similares; encorajá-los a levar o fraudador à Justiça; cooperar com sua investigação e processo judicial.

- Entrar em litígio civil ou processos legais similares para recuperar a quantia levada.

- Abrir um sinistro junto à seguradora.

- Fazer uma reclamação junto à associação profissional do perpetrador.

- Recomendar melhorias nos controles.

F. Comunicações de Incidentes de Fraude

Além do reporte de fraude mencionado anteriormente, os dois tipos de comunicações que podem resultar de uma investigação são comunicações públicas e comunicações internas planejadas.

A gerência ou o conselho determina se deverão ser informadas as entidades externas à organização, após consulta com indivíduos, tais como o conselheiro legal, pessoal de recursos humanos e o DEA. A organização pode ter a responsabilidade de notificar agências do governo acerca de certos tipos de atos fraudulentos. Essas agências incluem a polícia, agências regulatórias ou órgãos supervisores. Além disso, a organização pode ter a obrigação de notificar as seguradoras, bancos e auditores externos da organização, acerca dos casos de fraude. Quaisquer comentários feitos pela gerência à imprensa, polícia ou partes externas são melhor coordenados por meio do conselheiro legal. Tipicamente, apenas porta-vozes autorizados fazem comunicações e comentários externos.

Uma decisão importante neste processo é a decisão de processar o fraudador. Esta decisão é tomada pela gerência e pelo conselho, normalmente com base na contribuição do conselheiro legal. Embora os auditores internos não tomem tais decisões, eles podem informar à gerência e ao conselho que processos judiciais desencorajam novas fraudes, por reforçar as repercussões do comportamento fraudulento e, portanto, servem para a dissuasão da fraude.

As comunicações internas são uma ferramenta estratégica usada pela gerência para reforçar sua posição com relação à integridade, para demonstrar que toma as ações apropriadas (incluindo processos judiciais, quando apropriado), quando a política da organização é violada e para mostrar por que os controles internos são importantes. Tais comunicações tomam forma de artigo em *newsletters*, um memorando da gerência ou a situação pode ser usada como exemplo no programa de treinamento contra fraude da organização. Estas comunicações geralmente ocorrem após o caso ter sido resolvido internamente e não especificam nomes de fraudadores ou outros detalhes específicos da investigação que não sejam necessários para a mensagem ou que se oponham à lei. Uma investigação e seus resultados podem causar um estresse significante ou questões de moral que podem perturbar a organização, especialmente quando a fraude vai a público. A gerência pode planejar sessões com os funcionários e/ou estratégias de formação de equipe para retomar a confiança e camaradagem entre os funcionários.

G. Análise das Lições Aprendidas

Depois que a fraude for investigada e comunicada, é importante que a gerência e a atividade de auditoria interna deem um passo atrás e considerem as lições aprendidas. Por exemplo:

- Como a fraude ocorreu?
- Quais controles falharam?
- Quais controles foram sobrepostos?
- Por que a fraude não foi detectada antes?
- Quais *red flags* não foram percebidos pela gerência?
- Quais *red flags* não foram percebidos pela auditoria interna?
- Como fraudes futuras podem ser prevenidas ou detectadas mais facilmente?
- Quais controles precisam ser fortalecidos?
- Quais planos de auditoria interna e passos de auditoria precisam ser melhorados?
- Qual treinamento adicional é necessário?

Tanto a gerência quanto os auditores internos podem conduzir sessões para debater as lições aprendidas. O *feedback* dinâmico nessas sessões precisa destacar a importância da obtenção de informações atualizadas sobre fraudadores e esquemas de fraude que possam ajudar os auditores internos e a comunidade antifraude a se envolver nas melhores práticas para prevenir perdas.

As políticas e procedimentos de fraude da gerência definem quem tem a autoridade e a responsabilidade por cada aspecto do processo. A atividade de auditoria interna pode estar envolvida como conselheiros no processo, desde que o impacto dessas atividades sobre a independência da auditoria interna seja reconhecido e abordado apropriadamente. Além de aconselhar a gerência, os auditores internos podem se envolver nas investigações:

- Monitorando o processo de investigação para ajudar a organização a seguir políticas e procedimentos relevantes, além de leis e estatutos aplicáveis (quando a auditoria interna não for responsável por conduzir a investigação).
- Localizando e/ou protegendo ativos apropriados indevidamente ou relacionados.
- Apoiando os processos legais, sinistros e outras ações de recuperação da organização.
- Avaliando e monitorando o reporte interno e externo pós-investigação da organização e seus planos e práticas de comunicação.
- Monitorando a implementação das recomendações de melhorias dos controles.

Os auditores internos tipicamente avaliam os fatos das investigações e aconselham a gerência, com relação à resolução das fraquezas de controle que levem à fraude. Os auditores internos podem desenvolver passos em programas de auditoria ou desenvolver programas de "auditorias para fraude", para ajudar a divulgar a existência de fraudes similares no futuro.

Formando uma Opinião sobre os Controles Internos Relacionados à Fraude

A gerência ou o conselho pode pedir ao auditor interno que dê sua opinião sobre o sistema de controles internos relacionados à fraude da organização. Veja as publicações a seguir para mais informações sobre este tópico:

- Práticas Recomendadas do IIA, da série 2410.
- Guia Prático do IIA, *Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Controls*.

Anexo A – Material de Referência

The Institute of Internal Auditors (IIA), Prática Recomendada 1210-1: Proficiência, www.theiia.org

The IIA, Prática Recomendada 1210.A1-1: Obtenção de Prestadores Externos de Serviços para Apoiar ou Complementar a Atividade de Auditoria Interna, www.theiia.org

The IIA, Prática Recomendada 1220-1: Zelo Profissional Devido, www.theiia.org

The IIA, Prática Recomendada 2030-1: Gerenciamento de Recursos, www.theiia.org

The IIA, Prática Recomendada 2060-1: Reporte à Alta Administração e ao Conselho, www.theiia.org

The IIA, *Joining the Fight Against Corruption*, 2009, www.theiia.org

The IIA, *The Role of Internal Auditing in Preventing and Detecting Misuse, Fraud, and Bribery*, Patty Miller, Fevereiro de 2007

The IIA, *SOX Section 404: A Guide for Management by Internal Controls Practitioners*, 2ª edição, The IIA, 2008, www.theiia.org

Fundação de Pesquisa do IIA, *Using Non-Financial Measures to Assess Fraud Risk*, Brazel, Jones e Zimbelman, Agosto de 2008, www.theiia.org

Internal Auditor Magazine, "Fraud Risk Assessment," Jonny Frank, Abril de 2004, www.internalauditoronline.org

Internal Auditor Magazine, "4 Steps to a Successful Fraud Risk Assessment," Paul Zikmund, Fevereiro de 2008, www.internalauditoronline.org

Internal Auditor Magazine, "The Risk Matrix Revisited," Larry Hubbard, Abril de 2009, www.internalauditoronline.org

Internal Auditor Magazine, edição *Focusing on Fraud*, Outubro de 2009, www.internalauditoronline.org

Contabilidade Pública

American Institute of Certified Public Accountants (AICPA), "The Auditor's Responsibility for Fraud and the Importance of Professional Skepticism," 2008, www.aicpa.org

Deloitte, Fraud & the Regulatory Environment, Stefan DuChene, Março de 2006, https://www.tmaccalgary.com/presentation/Stefan%20DuChene.ppt

KPMG LLP, *Profile of a Fraudster Survey 2007*, www.us.kpmg.com

KPMG LLP, *Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response*, 2006, www.us.kpmg.com

PricewaterhouseCoopers (PwC), *Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-centric Approach*, 2007, www.pwc.com

Association of Certified Fraud Examiners (ACFE)

The Association of Certified Fraud Examiners (ACFE)/*American Institute of Certified Public Accountants* (AICPA), *Fraud Tools*, www.acfe.com

ACFE, 2008 ACFE *Report to the Nation on Occupational Fraud & Abuse*, 2008, www.acfe.com

ACFE, "How Fraud Hurts You and Your Government Organization," http://www.acfe.com/resources/fraudtools.asp?copy=video

ACFE "Sample Fraud Policy," http://www.acfe.com/documents/sample_fraud_policy.pdf

Documentos Conjuntos

The IIA, ACFE e AICPA, *Managing the Business Risk of Fraud: A Practical Guide*, 2008, www.theiia.org

The IIA, ACFE, *Information System Accountability and Control Auditors*, *Financial Executives Institute*, *Institute of Management Accountants* e *Society of Human Resource Professionals*, "Management Anti-Fraud Programs and Controls: Guidance to Help Prevent, Deter, and Detect Fraud", 2002

Outros

Howard Silverstone e Howard Davia, *Fraud 101: Techniques and Strategies for Prevention* (2ª Edição), 2005

Anexo B – Perguntas a Considerar

Conduzir discussões oportunas e apropriadas sobre fraude com todos os níveis da organização, incluindo o comitê de auditoria, demonstra o papel proativo que a atividade de auditoria interna está desempenhando em sua área. Algumas das perguntas que os auditores internos podem fazer regularmente sobre fraude incluem:

1. A organização tem uma estrutura de governança de fraude em prática que designe responsabilidades pelas investigações de fraude?
2. A organização tem uma política contra fraude em prática?
3. A organização identificou leis e regulamentos relacionados à fraude, nas jurisdições em que tem negócios?
4. O programa de gerenciamento de fraudes da organização inclui a coordenação com a auditoria interna?
5. A organização tem um canal de denúncias de fraude?
6. O estatuto de auditoria descreve os papéis e responsabilidades da auditoria interna, com relação à fraude?
7. A responsabilidade pela detecção, prevenção, resposta e conscientização contra fraude foi designada dentro da organização?
8. A gerência e o DEA mantêm o comitê de auditoria informado sobre fraudes?
9. A gerência promove a conscientização e treinamento contra fraude, dentro da organização?
10. A gerência lidera avaliações do risco de fraude e inclui a auditoria interna no processo de avaliação?
11. Os resultados das avaliações do risco de fraude são considerados no processo de planejamento de auditoria?
12. Programas periódicos de conscientização e treinamento contra fraude são oferecidos a todos os funcionários?
13. Há ferramentas automatizadas disponíveis para aqueles responsáveis pela prevenção, detecção e investigação de fraude?
14. A gerência identificou os tipos de riscos de fraude em potencial em suas áreas de responsabilidade?
15. A gerência e o DEA sabem onde obter orientações sobre fraude por parte de organizações profissionais?
16. A gerência e os auditores internos conhecem suas responsabilidades profissionais, com relação à fraude?
17. A gerência incorporou os controles apropriados para prevenir, detectar e investigar fraudes?
18. A gerência tem em prática os conjuntos de habilidades necessários para conduzir investigações de fraude?
19. A gerência e a atividade de auditoria interna avaliam periodicamente a eficácia e a eficiência dos controles de fraude?
20. Os papéis de trabalho de investigações de fraude e documentos de apoio ficam apropriadamente protegidos e retidos?

Observação: Esta lista não é um *checklist*. Ela não inclui todas as perguntas que podem ser necessárias para avaliar os riscos de fraude em uma organização, nem contém as perguntas de acompanhamento necessárias que dependem das respostas a perguntas anteriores. Portanto, os auditores podem usá-la para começar a desenvolver suas próprias ferramentas e para conduzir um *brainstorming* sobre riscos de fraude.

Anexo C – Modelo de Avaliação do Risco de Fraude

Esta tabela serve como um modelo ilustrativo de uma avaliação do risco de fraude. A personalização ou ajuste é necessário para adaptá-la à avaliação do risco de fraude em sua organização.

Proprietário	Riscos de Fraude	Controles	Monitoramento	Probabilidade	Impacto
Departamento de Construção	Conluio entre empreiteiro e subempreiteiro. • Cartel em Licitação • Suborno/ Propinas	• Qualificação dos empreiteiros antes da licitação (solvência financeira, reputação). • Procedimentos formais de licitação competitiva são usados na seleção de um empreiteiro geral (*general contractor* – GC). Exemplo: Propostas Fechadas. • Seleção do subempreiteiro: Para todo o trabalho acima do limite de $, a licitação competitiva é exigida pelo GC. • Cartas de confirmação de proposta são enviadas aos subempreiteiros para garantir a integridade do processo de licitação. • Verificação do histórico, incluindo pesquisas de fraudes passadas ou violações de ética. Além disso, pedir ao GC para assinar a Declaração de Ética. • Auditorias internas periódicas são realizadas para projetos selecionados, para determinar a conformidade com o contrato e buscar irregularidades.	• Departamento de Construção • Compras • Jurídico • Auditoria Interna	M	M

Proprietário	Riscos de Fraude	Controles	Monitoramento	Probabilidade	Impacto
Departamento de Construção	Defeitos de design e construção (material inferior usado e construção não realizada de acordo com as especificações). • Risco de reputação (lesões ou fatalidades no local).	• Executar o contrato de construção com escopo detalhado de trabalho (especificações). • Visitas periódicas de arquitetos, inspetores prediais locais, engenheiros, agentes comissionados e representantes do proprietário ao local da obra são realizadas para garantir que o trabalho esteja em dia e realizado de acordo com as especificações e o código. • Exibir o número do canal de denúncias de fraude no local. • Auditorias internas periódicas são realizadas para projetos selecionados, para determinar a conformidade com o contrato e buscar irregularidades.	• Departamento de Construção • Jurídico • Auditoria Interna	M	A

Proprietário	Riscos de Fraude	Controles	Monitoramento	Probabilidade	Impacto
Departamento de Construção	Superfaturamento do empreiteiro. • Preço • Quantidade • Cobranças em duplicidade • Faturas fictícias • Descontos de compra não creditados • Transações de parte relacionada.	• A gerência examina e aprova as faturas. • O acompanhamento dos custos é conduzido para monitorar as despesas de cada projeto e determinar razões para variações significantes, em relação ao orçamento de capital. • Pesquisar com precisão o excesso de custo e obter aprovação, antes de ajustar o preço do contrato. • Quaisquer mudanças no escopo de trabalho incluem uma avaliação da mudança por escrito, com revisão da gerência e aprovação, antes do início do trabalho. • Os avaliadores de construção do proprietário revisam os aumentos de custos ou créditos para precisão e competitividade. • O contrato declara que transações de parte relacionada ou afiliados devem ser divulgadas e aprovadas pelo proprietário. Os relatórios de crédito são obtidos ou pesquisas online são feitas aleatoriamente. • Exibir o número do canal de denúncias de fraude no local. • Auditorias internas periódicas são realizadas para projetos selecionados, para determinar a conformidade com o contrato e buscar irregularidades.	• Departamento de Construção • Comitê de Apropriação de Capital • Jurídico • Avaliador • Controllers • Auditoria Interna	M	M

Proprietário	Riscos de Fraude	Controles	Monitoramento	Probabilidade	Impacto
Departamento de Construção	Incapacidade de trabalho	• Liberação da Caução do Empreiteiro assinada e autenticada é necessária, antes de liberar fundos ao empreiteiro. • Obter Garantia de Execução, caso o empreiteiro não cumpra com suas obrigações contratuais. • Uma porção do pagamento devido (retenção) não é paga ao empreiteiro, até que 100% do trabalho seja concluído e as liberações de caução finais sejam recebidas. • Exibir o número do canal de denúncias de fraude no local. • Auditorias internas periódicas são realizadas para projetos selecionados para determinar a conformidade com o contrato e buscar irregularidades.	• Departamento de Construção • Controllers • Auditoria Interna	M	B
Departamento de Construção	Defeitos de design e construção (material inferior usado e construção não realizada de acordo com as especificações). • Risco de reputação (lesões ou fatalidades no local).	• Proprietário designa um gerente de projeto no local para monitorar o trabalho. • O representante do proprietário no local supervisiona os procedimentos para controlar o equipamento e materiais do local. • Contratação de seguranças para o local. • Exibir o número do canal de denúncias de fraude no local. • Auditorias internas periódicas são realizadas para projetos selecionados para determinar a conformidade com o contrato e buscar irregularidades.	• Departamento de Construção • Auditoria Interna	A	B

Autores:

- Gregory S. Dubis, CIA, CCSA, CISA, CFE
- Abraham D. Akresh, CPA, CGFM
- Princy Jain, CIA, CCSA, CFE e CA (Índia)
- Lynn Morley, CIA CGA
- Theresa M. Phipps, CPA
- Richard A. Schmidt, CPA, CIA, CFE

Revisores e Colaboradores:

- Douglas J. Anderson, CIA, CPA
- Steve Hunt, CIA, CISA, CGEIT, CBM
- Ken Askelson, CIA, CPA, CITP
- Rich Lanza, CIA, CFE, PMP
- Peter Millar
- Marilyn Prosch, Ph.D.
- Donald E. Sparks, CIA, CISA, ARM

Sobre o Instituto

Fundado em 1941, *The Institute of Internal Auditors* (IIA) é uma associação profissional com sede global em Altamonte Springs, Fla., EUA. O IIA é a voz da profissão de auditoria interna em todo o mundo, autoridade reconhecida, líder valorizado, advogado chefe e principal educador.

Sobre os Guias Práticos

Os Guias Práticos fornecem uma orientação detalhada para a condução de atividades de auditoria interna. Eles incluem processos e procedimentos detalhados, como ferramentas e técnicas, programas e abordagens passo-a-passo, assim como exemplos de *deliverables*. Os Guias Práticos são parte da IPPF do IIA. Como parte da categoria de orientação Fortemente Recomendada, a conformidade não é obrigatória, mas é altamente recomendada, e a orientação é endossada pelo IIA por meio de processos formais de revisão e aprovação.

Para mais materiais de orientação fidedignos fornecidos pelo IIA, por favor, visite nosso website: www.theiia.org/guidance

Disclaimer

O IIA publica este documento para fins informativos e educacionais. Este material de orientação não tem como objetivo fornecer respostas definitivas a específicas circunstâncias individuais e, como tal, tem o único propósito de servir de guia. O IIA recomenda que você sempre busque conselhos especializados independentes, relacionados diretamente a qualquer situação específica. O IIA não assume responsabilidade pela confiança depositada unicamente neste guia.

Copyright