GLOBAL PERSPECTIVES & INSIGHTS

FRAUDE

PARTE I: Fraude na Criptosfera

PARTE 2: Auditores Internos e Examinadores de Fraude: Uma Parceria Valiosa

PARTE 3: A Ressaca: Fraude na Era Pós-COVID

The Institute of Internal Auditors

Conteúdos

Parte 1

Fraude na Criptosfera

Sobre os Especialistas

Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Dana Lawrence é *Chief Compliance Officer* da Fideseo. É uma especialista reconhecida e líder em conformidade complexa, gerenciamento de riscos corporativos (ERM), auditoria interna e criação, escalação e correção de programas de governança. A carreira de Lawrence em tecnologia e serviços financeiros abrange hipotecas, bancos comunitários, grandes bancos americanos e globais, parceiros de *open banking*, *fintech* e cripto. Ocupou cargos da alta liderança, trabalhando diretamente com reguladores bancários e auditores internos/externos. Lawrence é uma escolha popular como oradora e anfitriã de eventos, tendo palestrado em eventos locais, nacionais e globais com até 40.000 participantes. É uma voluntária e líder criativa comprometida, servindo a vários grupos, como o The IIA.

Lourdes Miranda, CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

Lourdes Miranda é *Chief Compliance Officer* da SendCrypto, uma empresa de tecnologia *blockchain*. Já foi agente da CIA e analista do FBI e tem mais de 20 anos de experiência corporativa e governamental, especializada em investigações de crimes financeiros e coleta e análise de inteligência globalmente. Tem vasta experiência de campo, com foco em lavadores de dinheiro e financiadores de terroristas. Desde 2017, Miranda trabalha para *FinTechs* como investigadora sênior de cripto, *senior compliance officer* e gerente de riscos, criando equipes e programas de treinamento de compliance, investigação, cripto e inteligência. Também é autora, instrutora e colaboradora de vários cursos on-line como especialista. Além disso, Miranda é membro do Conselho Consultivo da *Toronto Compliance & AML Enterprise* (TCAE), com sede no Canadá.

Introdução

Criptomoedas e fraudes na conversa global

Sam Bankman-Fried, o carismático fundador da *exchange* de criptomoedas FTX, já teve uma fortuna estimada em US$ 26,5 bilhões. Como líder do que já foi a terceira maior bolsa no mercado de criptomoedas, Bankman-Fried e FTX eram os queridinhos de uma variedade de investidores de alto nível, como BlackRock e o jogador da NFL Tom Brady. No entanto, ele perdeu toda a sua riqueza praticamente da noite para o dia, em um dos colapsos de empresas mais dramáticos da história moderna.

Bankman-Fried foi preso em 13 de dezembro de 2022, nas Bahamas. De acordo com relatórios publicados, ele encara várias acusações, incluindo fraude eletrônica, conspiração de fraude eletrônica, fraude de valores mobiliários, conspiração de fraude de valores mobiliários e lavagem de dinheiro.

Embora haja um interesse humano no simples espetáculo de uma queda tão incrível, o evento também levantou questões maiores em relação aos ativos digitais. Com paralelos a escândalos como Tornado Cash e Bitzlato, o colapso da FTX e o impacto subsequente na indústria que ela representava levou muitos a questionar a viabilidade de longo prazo dos criptoativos — pelo menos em seu estado atual, que o presidente da Comissão de Valores Mobiliários dos EUA Gary Gensler chamou de "Velho Oeste".

Apesar de construída com base na tecnologia *blockchain*, que está entre as formas mais seguras de manter ativos e informações criptográficas, se o chefe tão visível de uma das bolsas de criptomoedas mais proeminentes do mundo puder supostamente cometer atos de fraude em larga escala, que outras vulnerabilidades podem existir para empresas que operam na indústria de alguma forma? Como o cenário de riscos mudou com o aumento meteórico dos criptoativos e como algumas organizações e suas funções de auditoria interna estão respondendo com sucesso a essas mudanças?

A Parte 1 desta série de três partes sobre fraude abordará essas questões, examinando os esquemas de fraude comuns vistos nos estágios iniciais de um mundo de criptoativos. Para obter mais informações sobre esse tópico, o The IIA apresentará uma reprise de seu recente webinário *"Fraud perspectives: Blockchain, Crypto, and KYC"*, com uma sessão de perguntas e respostas ao vivo com os especialistas citados neste *Brief*.

Incerteza na Criptosfera

Um futuro empolgante, mas arriscado

As organizações agora estão prestando atenção

Embora suas implicações sejam vastas e essencialmente revolucionárias, a tecnologia *blockchain* é relativamente fácil de entender conceitualmente como nada mais do que um registro contínuo e crescente de transações de ativos digitais que podem ser compartilhados e armazenados em praticamente qualquer estrutura de rede. O que a diferencia é que ela usa metodologias de verificação que criptografam continuamente o bloco a cada nova transação, tornando-o mais seguro.

"A tecnologia em si é extremamente complicada e leva anos de treinamento e educação para analisar, mas penso na *blockchain* em si como uma demonstração financeira", disse Lourdes Miranda, *chief compliance officer* da SendCrypto, uma empresa de tecnologia *blockchain*. "A *blockchain* tem informações sobre quem enviou os ativos, onde foram depositados, se houve saques e o saldo resultante."

A criptomoeda é indiscutivelmente o ativo mais conhecido que utiliza essa tecnologia, criando um sistema (ou sistemas) monetário descentralizado e de código aberto imune à influência de entidades, como bancos centrais — mas outros exemplos de criptoativos baseados em *blockchain* incluem tokens não fungíveis *(non-fungible tokens* – NFTs), tecnologias de contabilidade distribuída *(distributed ledger technologies* – DLTs), tokens de jogos, entre outros.

No entanto, como as indústrias estão aprendendo rapidamente, não é porque os criptoativos são construídos em tecnologia segura, praticamente impossível de manipular pelos métodos tradicionais, que seus adotantes estejam imunes ao risco. O colapso da FTX ilustra isso de várias formas. Por exemplo, ilustrou como a falta de governança corporativa adequada e de controles internos pode ser prejudicial, não apenas para a organização, mas para os investidores em todo o cenário da indústria.

Esse foi um argumento que o presidente e CEO do IIA, Anthony Pugliese, apresentou em uma carta recente ao Congresso dos EUA que pedia que estabelecessem novos requisitos para reforçar a governança corporativa em *exchanges* de criptomoedas, empresas de tecnologia *blockchain*, mercados de NFT e plataformas Web3 operando nos Estados Unidos. "Inúmeros investidores estão agora pagando o preço pelas falhas da FTX", disse Pugliese. "Está claro que não podemos confiar que exchanges não regulamentadas farão a coisa certa por conta própria – precisamos impor normas mais fortes de governança corporativa e garantir a prestação de contas quando a *exchange* não estiver protegendo seus clientes. Quando os malfeitores corporativos são pegos, não deveria sobrar para os investidores."

Pugliese enfatizou que o colapso da FTX e suas consequências no mercado poderiam ter sido mitigadas por meio de ações de uma função sólida de auditoria interna. "O colapso da FTX é o mais recente lembrete de que organizações sem uma função robusta de auditoria interna estão, na melhor das hipóteses, brincando com fogo e, na pior, preparando a si mesmas e a seus stakeholders para uma queda desastrosa – e totalmente evitável", disse ele.

As preocupações de Pugliese e de outros foram ouvidas. Em 3 de janeiro de 2023, a *Federal Reserve, Federal Deposit Insurance Corp* (FDIC) e o *Office of the Comptroller of the Currency* (OCC) divulgaram sua primeira declaração conjunta sobre criptomoedas. Nela, destacaram uma variedade de riscos que podem estar em jogo para organizações bancárias que operam em criptomoeda de alguma forma, incluindo:

- Risco de fraude e golpes entre os participantes do setor de criptoativos.
- Incertezas legais relacionadas a práticas de custódia, resgates e direitos de propriedade.
- Representações e divulgações imprecisas ou enganosas por empresas de criptoativos.
- Volatilidade significativa nos mercados de criptoativos, cujos efeitos incluem impactos potenciais nos fluxos de depósitos associados a empresas de criptoativos.
- Risco de contágio no setor de criptoativos, resultante de interconexões entre certos participantes de criptoativos, inclusive por meio de empréstimos opacos, investimentos, financiamento, serviços e acordos operacionais.
- Práticas de gerenciamento de riscos e governança no setor de criptoativos sem maturidade e robustez.
- Riscos elevados associados a redes abertas, públicas e/ou descentralizadas ou sistemas semelhantes.

Embora todos esses riscos sejam dignos de discussão (e, em muitos casos, aplicáveis a organizações além dos bancos interessados em cripto), este *Brief* limitará o foco a atos de fraude cometidos em participantes de cripto e as formas proeminentes que assumem no ambiente atual.

Um Cenário Propício à Fraude

Um cenário de risco em constante expansão

Uma nova ferramenta para o malfeitor

Embora os criptoativos tenham uma série de características vantajosas, como transparência e criptografia notavelmente avançada contra manipulação, essas mesmas características tornaram esses ativos (e a tecnologia *blockchain* por trás deles) uma ferramenta poderosa para quem deseja cometer fraudes.

De fato, é esse apelo aos malfeitores que chamou a atenção dos reguladores e das autoridades policiais. "A única razão pela qual os regulares se preocupam com criptoativos é porque malfeitores os estão usando para financiar operações e lavar dinheiro", disse Miranda, que pesquisou crimes financeiros para a CIA e o FBI por quase 30 anos. "A *blockchain* é muito difícil de manipular, mas pode ser utilizada de forma a promover atividades nefastas."

Um método, por exemplo, é o uso de identidades falsas de identificação dentro da *blockchain*. "Isso é enorme na criptosfera", disse Miranda. "Malfeitores usarão identidades legítimas e válidas compradas no mercado negro para passar no processo de *onboarding* KYC *[Know Your Customer]* quando as carteiras são abertas. Essas identidades não têm antecedentes criminais e não estão em qualquer lista negra — são completamente limpas. Então, com esse nome limpo, eles podem movimentar dinheiro sem ser detectados, até que os investigadores possam ver as tendências de fraude com seus próprios olhos."

A indústria de criptoativos também apresentou uma variedade de ferramentas que, embora criadas para a conveniência do consumidor, possuem uma variedade de brechas que podem ser exploradas. Um iniciador de fraude, por exemplo, pode fazer uso de um hub de transações criptográficas, como um caixa eletrônico Bitcoin, junto com um celular descartável para evitar rastreio por parte das autoridades.

"Digamos que eu estou em Nova York e quero movimentar dinheiro em finanças, e tenho que pagar meus malfeitores em Miami. Eles querem ser pagos, e rapidamente. Não vou receber um cheque e não posso usar um computador ou laptop, porque o endereço IP é rastreável, então, o que eu faço é ir a um caixa eletrônico Bitcoin em Nova York e usar dinheiro em espécie e um celular descartável. Dessa forma, posso pagar as pessoas, enquanto contorno os protocolos de combate à lavagem de dinheiro. Isso é fraude", disse Miranda.

Pig butchering

Outra tática comum de fraude que os malfeitores podem utilizar é conhecida pelo termo gráfico *"pig butchering"* ("abate de porcos"). "É basicamente o conceito de um fraudador metaforicamente 'engordar' sua vítima, investindo muito tempo nela para estabelecer confiança", disse Dana Lawrence, *chief compliance officer* da empresa de consultoria de negócios e tecnologia Fideseo. O tempo investido pelos fraudadores pode acontecer em qualquer lugar, de acordo com Lawrence, mas é feito mais frequentemente nas redes sociais ou por meio de mensagens de texto ao longo de semanas ou meses. Lawrence citou o LinkedIn especificamente como uma plataforma favorita, bem como sites sociais como o Twitter.

Nesses casos, o malfeitor normalmente se apresentará como um influenciador ou *insider* que investiu com sucesso em criptomoedas. Com o tempo, divulgarão os benefícios da criptomoeda em um esforço para fazer com que a vítima transfira seus ativos para eles. Em alguns casos, os fraudadores fornecem à vítima demonstrações financeiras falsas, para fazer parecer que retornos substanciais estão sendo obtidos.

Embora seja fácil ler esses sinais e considerá-los relativamente óbvios de se identificar, os fraudadores que usam esta técnica tornaram-se altamente sofisticados. Equipes de golpistas em países como Camboja e China, por exemplo, receberam treinamento aprofundado de psicólogos sobre como tornar as pessoas mais vulneráveis a tomar decisões erradas.

"Foram treinados por psicólogos para tentar descobrir a melhor forma de manipular as pessoas", disse o promotor distrital do condado de Santa Clara, Califórnia, Jeff Rosen, em entrevista à CNN. "Você está lidando com pessoas que usarão diferentes técnicas psicológicas para torná-lo vulnerável e fazer com que você se interesse em abrir mão do seu dinheiro."[1]

Pump and dump

A outra grande forma de fraude vista na criptosfera é bem conhecida por observadores de longa data do mercado de ações: o chamado esquema *"pump and dump"*.

"Esse esquema geralmente começa com um grupo se reunindo para iniciar um novo projeto criptográfico, como um token e, então, usando – geralmente com a ajuda de influenciadores – recursos para promovê-lo em plataformas como Twitter ou Discord", disse Lawrence. "Atualmente, há muita flutuação no mercado de criptomoedas devido à liquidez. Portanto, se muitas pessoas tentarem comprar algo de uma só vez, isso meio que choca o mercado, fazendo-o aumentar o preço. Se isso acontecer, os malfeitores em questão, que detêm grandes quantidades do ativo, rapidamente o vendem com lucro, baixando o preço repentinamente e deixando todos os outros investidores com algo que vale essencialmente zero".

O alerta vermelho nessas situações, disse Lawrence, é uma clara falta de divulgações que indiquem aos potenciais investidores que perder tudo é uma possibilidade distinta. Os malfeitores também costumam fazer uso intenso de mensagens copiadas e coladas nas redes sociais e fóruns de discussão, publicadas por autores com nomes de usuário semelhantes. E, depois que o esquema é perpetrado, esses nomes de usuário geralmente desaparecem, preservando seu anonimato completamente intacto.

Outros exemplos de fraude em um contexto de criptoativos

A fraude baseada em criptografia nem sempre precisa ser tão sofisticada. Dentro das organizações baseadas em criptografia, muitas vezes tudo o que é necessário para um malfeitor é a oportunidade certa. Por exemplo, embora a própria *blockchain* mantenha os ativos digitais seguros, tudo o que é necessário para burlar a segurança e esvaziar uma carteira criptográfica é obter uma chave privada – uma longa sequência de números que cabem em um guardanapo de restaurante e podem ser deixados em qualquer lugar para qualquer um encontrar.

"Sua chave privada é sua identidade digital no mercado de criptomoedas, e qualquer um que se apossar dela pode realizar transações fraudulentas ou roubar suas criptomoedas", disse Lawrence. "Se alguém de alguma forma, obtiver acesso a ela, não há nada que eu possa fazer a respeito. Não posso recuperá-la, não posso registrar uma reclamação, não há qualquer agência de proteção ao consumidor ou regulador junto ao qual eu possa contestar – está literalmente perdida."

Com o amadurecimento do mercado criptográfico, surgiram serviços de criptosegurança especializados em proteger chaves individuais e corporativas contra extravio, mas, em alguns casos, suas metodologias são surpreendentemente primitivas. Segundo Lawrence, a solução aplicada por alguns desses serviços é guardar as chaves em cofres na encosta de montanhas desertas. O seguro cripto também existe como rede de segurança para as empresas que podem pagar, mas, neste estágio, toda a indústria está tendo dificuldades quanto à lucratividade, forçando as seguradoras a ser incrivelmente seletivas e, ao mesmo tempo, oferecer uma cobertura que diminui a cada ano.

1. Josh Campbell, "Beware the 'Pig Butchering' Crypto Scam Sweeping Across America", 26 de dezembro de 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.

Em um artigo publicado no *Insurance Times* do Reino Unido, o sócio do grupo RPC Insurance, James Wickes, discutiu os desafios do mercado de seguros cripto. "O número relativamente pequeno de seguradoras atualmente ativas no âmbito de seguros de criptoativos provavelmente estará interessado em revisar as letras miúdas das apólices, para limitar a exposição potencial à volatilidade dos mercados criptográficos, conforme demonstrado pelo recente *crash*", disse. "O mercado de seguros para esses ativos está em sua infância e resta saber se um conjunto suficiente de seguradoras estará preparado para fornecer capacidade suficiente para atender à demanda e quão corajoso o mercado será para estender a cobertura além do risco de roubo tradicional."[2]

Apesar dessas precauções, no entanto, ainda há certas ferramentas que os malfeitores podem usar para ainda utilizar criptoativos e *blockchain* sem contornar diretamente uma conta estabelecida – ou seja, *mixers*, também conhecidos como *tumblers*. Um dos principais recursos de *blockchain* é sua transparência; dentro de qualquer explorador de *blockchain*, qualquer pessoa pode visualizar o registro de todas as transações de *blockchain* desde o lançamento da criptomoeda em 2009. Os *mixers* permitem que o usuário essencialmente misture a quantidade de criptoativos em questão antes de entregá-los aos destinatários pretendidos, dando-lhes um grau de anonimato, já que é tão difícil decifrar exatamente quem enviou quantos ativos para quem. Usando um *mixer*, tudo o que um explorador mostrará é que uma pessoa, assim como dezenas de outras pessoas, enviou ativos para um *mixer* e, em seguida, enviou os ativos em quantidades variadas para uma variedade de outras pessoas. O resultado, em essência, assemelha-se a uma forma aperfeiçoada de lavagem de dinheiro.

Diante dessas realidades, as organizações que optam por existir na criptoesfera devem aceitar que estão, em grande parte, por conta própria quando se trata da mitigação de riscos neste estágio. Isso não significa que a criptografia deva ser evitada, mas significa que a conformidade, o controle interno sólido, os esforços de detecção e dissuasão de fraudes e a auditoria interna devem desempenhar um papel importante nas conversas sobre criptografia do nível do conselho para baixo.

2. Isobel Rafferty, "Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments", *Insurance Times*, 18 de julho de 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

Onde a Auditoria Interna Pode Começar

A regulação chegou, e mais está por vir

Recursos de orientação emitidos

Conforme mencionado anteriormente, são escassos os frameworks regulatórios que as empresas podem buscar para lidar com segurança e governança quanto a criptoativos e riscos associados à fraude. No entanto, certas indústrias, como serviços financeiros, não são totalmente desprovidas de recursos que abordam os princípios de governança adequados em relação à proteção de ativos digitais — muitos dos quais são aplicáveis à criptomoeda.

Em outubro de 2022, a União Europeia apresentou o conteúdo acordado da *The Markets in Crypto-Assets* (MiCA) *Regulation*, que é uma das primeiras tentativas globais de regulamentação abrangente do marketing de criptomoedas, embora a legislação tenha sido adiada até abril de 2023, para que seja traduzida para 24 idiomas diferentes. Caso seja formalmente adotado, o regulamento:

- Define oficialmente o criptoativo como "uma representação digital de valor ou direitos que podem ser transferidos e armazenados eletronicamente, usando tecnologia de contabilidade distribuída ou tecnologia semelhante". Além disso, oferece quatro categorias diferentes de criptoativos: tokens referenciados a ativos, tokens de *e-money*, tokens utilitários e uma quarta categoria para criptoativos que não se enquadram nas outras três categorias.
- Responsabiliza oficialmente os provedores de cripto, se perderem os criptoativos dos investidores.
- Exige que participantes dos mercados de criptoativos declarem informações sobre sua pegada ambiental e climática.
- Sobrepõe-se à legislação atualizada sobre lavagem de dinheiro e encarrega a *European Banking Authority* (EBA) de manter um registro público de prestadores de serviços de criptoativos em não conformidade.
- Exige que os provedores de criptoativos tenham autorização para operar na UE.
- Fornece um framework forte aplicável a *"stablecoins"* (criptomoeda atrelada a um ativo de referência externo), que exigirá que cada detentor de *stablecoin* receba um *claim* a qualquer momento por parte do emissor, gratuitamente.

Nos Estados Unidos, uma declaração conjunta da *Federal Reserve*, *Federal Deposit Insurance Corporation* (FDIC) e do *Office of the Comptroller of the Currency* (OCC) oferece alguns recursos para empresas americanas, com orientações destinadas a ajudar "organizações bancárias a se envolverem em discussões robustas sobre supervisão de atividades relacionadas a criptoativos propostas e existentes."[3] Elas incluem:

- *OCC Interpretive Letter 1179 "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank."*
- *Federal Reserve SR 22-6/ CA 22-6: "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations."*
- *FDIC FIL-16-2022 "Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities."*

Estes dificilmente são os únicos recursos disponíveis. Após o colapso da FTX, a SEC também divulgou orientações que orientavam as empresas a divulgar seu envolvimento com empresas de commodities digitais.

3. "Joint Statement on Crypto-Asset Risks to Banking Organizations", *Board of Governors of the Federal Reserve System*, *Federal Deposit Insurance Corporation*, *Office of the Comptroller of the Currency*, 3 de janeiro de 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

O valor da educação

Supondo que seja adotada, a proposta de legislação da UE entrará em vigor em 2024, mas quase certamente não será a última. Conforme o cenário regulatório se desenvolve mês a mês, a ação mais valiosa que um auditor interno pode realizar é fazer todos os esforços para se manter a par das mudanças e articular claramente essas mudanças para o conselho e os stakeholders aplicáveis.

No ambiente atual, os auditores internos também devem articular aos stakeholders quais outras regulamentações existem que possam ser aplicáveis aos seus esforços de cripto. Por exemplo, disse Lawrence, uma empresa que oferece sua própria criptomoeda pode precisar de registro junto à *U.S. Financial Crimes Enforcement Network* — um detalhe crítico que pode ser facilmente esquecido, porque criptomoedas não são especificamente citadas na legislação. "Há muita incerteza agora", disse ela. "Cabe aos auditores internos informar aos líderes sobre o que é aplicável e o que não é."

O foco em novas tecnologias também não deve distrair as empresas das melhores práticas básicas quanto à proteção de ativos digitais, incluindo o uso de uma rede privada virtual (VPN) e segurança adequada, coleta e, quando necessário, descarte de informações de perfil de usuário — especialmente consumidores. "Os perfis de usuário são um controle organizacional crítico", disse Miranda. "Se eu estivesse auditando uma empresa, verificaria se os perfis de usuário correspondem à atividade transacional. Por exemplo, informações geográficas são incrivelmente importantes em conformidade e investigações. As organizações precisam manter essas informações seguras, bem como saber onde elas residem." Nesse ponto, Miranda observou que as organizações geralmente ignoram acordos de confidencialidade (NDAs), que contêm informações de perfil críticas, como endereços físicos, que podem ser essenciais para uma investigação de fraude.

Para mais informações, a Orientação Suplementar do IIA *"Internal Audit and Fraud: Assessing Fraud Risk Governance"* oferece orientação clara sobre os papéis e responsabilidades organizacionais para uma boa governança e gerenciamento do risco de fraude, bem como recomendações de orientações adicionais, como *Fraud Risk Management Guide* do COSO.

Conclusão

A auditoria interna está pronta

A criptomoeda e a tecnologia na qual ela se baseia são revolucionárias demais para ser ignoradas pela auditoria interna, com riscos que mais do que merecem a atenção do conselho. As avaliações de riscos que a ignoram têm um ponto cego crítico. A criptomoeda pode ser um conceito relativamente novo para muitos, mas não diminui o valor de um framework sólido de gerenciamento do risco de fraude, que possa ser mensurado e testado pela auditoria interna.

Embora seja fácil lamentar mais uma área de risco a ser adicionada ao radar cada vez maior da auditoria interna, a boa notícia é que nenhum outro departamento organizacional está em melhor posição para abordá-la. Assim como a lei Sarbanes-Oxley (SOX) fez em 2002, a evolução da regulamentação de criptomoedas praticamente garante à auditoria interna um lugar de valor à mesa nos próximos anos. Mesmo que a função ainda não tenha conhecimentos de cripto, ela tem conhecimento de fraude e de riscos; isso, por si só, é suficiente para preparar a auditoria interna para assumir uma posição de liderança ao enfrentar os desafios futuros.

Parte 2

Auditores Internos e Examinadores de Fraude: Uma Parceria Valiosa

Sobre os Especialistas

Mason Wilder, CFE

Mason Wilder é *Certified Fraud Examiner* e gerente de pesquisa da ACFE. Nessa função, supervisiona a criação e atualização de materiais da ACFE para educação profissional contínua, auxilia no planejamento e produção de todos os eventos de treinamento da ACFE, trabalha em iniciativas de pesquisa como o *Report to the Nations* e relatórios de *benchmarking*, realiza treinamentos, escreve para publicações da ACFE e responde a solicitações de membros e da mídia. Antes de ingressar na ACFE, Wilder trabalhou em inteligência e investigações de segurança corporativa por mais de uma década, especializando-se em investigações de antecedentes e *due diligence*, e análise de inteligência para segurança física internacional e resposta a crises. Mason construiu uma carreira coletando informações relevantes de todas as fontes, para analisar e destilar em apoio à tomada de decisões críticas, e é apaixonado por ajudar os profissionais antifraude a melhorar continuamente suas habilidades, para combater a fraude com eficácia.

Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB

Shawna Flanders, diretora de desenvolvimento de produtos do The Institute of Internal Auditors (IIA), é uma tecnóloga apaixonada e profissional do setor de treinamento técnico, com paixão por adaptar conversas técnicas à linguagem comercial comum. Shawna traz uma combinação única e complementar de habilidades para cada trabalho, incluindo: desenvolvimento/contribuição de conteúdo para SMEs, palestras/treinamentos, riscos relacionados a TI, auditoria de TI, segurança da informação e cibersegurança, conformidade de TI, governança de TI, gestão de fornecedores, generalista de TI em telecomunicações, programação, projeto/revisão de arquitetura relacionada a voz e dados, engenharia, análise e gestão de integração, gestão de processos de negócios, análise de negócios, gestão de projetos, gestão de programas e melhoria de processos/Six Sigma.

Introdução

Os auditores internos fornecem insights construtivos sobre governança, riscos e controles internos que ajudam as organizações a gerenciar riscos, incluindo a identificação e mitigação de fraudes. No entanto, embora a auditoria interna seja uma parte eficaz da detecção e dissuasão de fraudes, encontrar fraudes não é tarefa do auditor interno. Um *Certified Fraud Examiner* (CFE), por outro lado, é especificamente encarregado de identificar e investigar fraudes. O CFE traz habilidades especializadas para a batalha contra a fraude. Como resultado, faz sentido que os dois tipos de profissionais colaborem em uma parceria que atenda aos melhores interesses da organização.

Este Brief de Conhecimento Global, o segundo de uma série de três partes sobre fraude, examina os benefícios de construir um relacionamento simbiótico entre auditores internos e CFEs.

O Escopo da Fraude

Perda média de quase US$ 1,8 milhão

A fraude continua sendo um risco generalizado

Fraude é qualquer ato ilegal que envolva engano, ocultação ou violação de confiança que seja conduzido para ganho financeiro ou pessoal. As pessoas ou organizações que cometem fraudes podem estar tentando roubar dinheiro, propriedade ou serviços; evitar pagar ou perder algo; ou obter uma vantagem pessoal ou comercial. Além de golpistas externos, as fraudes também podem ser perpetradas por funcionários da empresa que estão passando por pressões financeiras ou que sentem que têm direito ao dinheiro ou aos serviços que "tomam", porque acham que a organização os tratou injustamente ou têm alguma outra reclamação. Qualquer tipo de organização pode ser vítima de fraude, não importando seu tamanho ou se é pública ou privada, sem fins lucrativos, órgão governamental ou de utilidade pública ou privada, ou outra entidade.

A fraude é um risco sério e generalizado para as organizações. As consequências da fraude podem variar de disruptivas a terríveis. Podem incluir não apenas desafios e perdas financeiras, mas também ineficiências que prejudicam operações, receitas ou lucros; cancelamento de projetos; e, dependendo de seu escopo, potencialmente o fracasso da organização.[4]

Uma pesquisa da *Association of Certified Fraud Examiners* (ACFE) com CFEs do mundo cobriu 2.110 casos de fraude em 133 países. Nesse grupo, as perdas globais devido a fraude totalizaram mais de US$ 3,6 bilhões, com uma perda média de quase US$ 1,8 milhão por caso. De fato, os CFEs estimam que as organizações perdem 5% de sua receita para fraudes todos os anos. Empresas menores claramente tiveram maior risco de fraude: aquelas com menos funcionários tiveram a maior perda mediana, de US$ 150.000.

Embora perdas desse tamanho possam ser fáceis de detectar, a fraude geralmente ocorre em incrementos menores ao longo do tempo. Um esquema típico de fraude pode resultar em uma perda de US$ 8.300 por mês e pode levar 12 meses para ser detectado, de acordo com a pesquisa. Também é importante estar ciente de que a criptomoeda está envolvida em algumas fraudes. A ACFE revelou envolvimento de criptomoedas em 8% dos casos. Os cenários usuais envolviam pagamentos de suborno e propina e conversão de ativos desviados.[5]

Categorias de Fraude Ocupacional

Há três categorias principais de fraude ocupacional, de acordo com o *Report to the Nations* de 2022 da ACFE.

Esquemas de fraude nas demonstrações financeiras, ou que causem uma distorção ou omissão relevante nas demonstrações financeiras da organização, foram os menos comuns (9%), mas os mais caros, com perdas de US$ 593.000 por caso.

A apropriação indébita de ativos, em que um funcionário rouba ou faz uso indevido de recursos da empresa, ocorreu em 86% dos casos. No entanto, foi responsável pelas menores perdas medianas: $ 100.000 por caso.

A corrupção, que abrange suborno, conflito de interesses e extorsão, esteve envolvida em 50% dos casos e levou a perdas de US$ 150.000 por caso.

Fonte: *Occupational Fraud 2022: A Report to the Nations*, ***Association of Certified Fraud Examiners.***

[4] Declaração de Posicionamento do IIA, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[5] *Occupational Fraud 2022: A Report to the Nations*, Association of Certified Fraud Examiners.

O Papel do Auditor Interno

Avaliação/assessoria sobre prevenção de fraudes

Detecção/dissuasão de fraude: um dos pilares da auditoria interna

De acordo com o *Institute of Internal Auditors* (IIA), "a auditoria interna é uma atividade independente e objetiva de avaliação e assessoria, criada para agregar valor e melhorar as operações de uma organização. Seu papel inclui detectar, prevenir e monitorar riscos de fraude, e lidar com esses riscos em auditorias e investigações."[6]

As organizações não devem esperar que o conjunto de habilidades da auditoria interna inclua investigação de fraude. Se as circunstâncias exigirem que a auditoria interna assuma uma função de investigação, os auditores internos devem exercer o zelo profissional devido e não devem prosseguir sem a experiência e o conhecimento necessários.

Embora a prevenção de fraudes seja função da gestão, a auditoria interna apoia os esforços antifraude da gestão, fornecendo os serviços de avaliação necessários sobre os controles internos criados para detectar e impedir fraudes. Frequentemente, a fraude ocorre devido a controles malfeitos e governança fraca, que prejudicam os processos da organização. Quase metade dos casos na pesquisa da ACFE foram atribuídos à falta de controles internos (29%) ou à capacidade de contornar os controles existentes (20%). Os auditores consideram o potencial de risco de fraude e a adequação dos controles internos nas áreas que examinam. Quando controles antifraude estão em vigor, tende a haver menos perdas por fraude e detecção mais rápida de fraude, de acordo com a pesquisa.

A contribuição da auditoria interna para os esforços antifraude não deve ser subestimada. Quando o IIA pediu aos chefes executivos de auditoria que citassem onde as funções de auditoria interna tiveram envolvimento significativo, 57% citaram fraude e 56% apontaram para a avaliação geral de riscos.[7] Enquanto isso, a pesquisa da ACFE constatou que a perda mediana por fraude era 50% maior (US$ 150.000 x US$ 100.000) quando não havia departamento de auditoria interna.

Considerações Integradas às Auditorias

Fonte: Relatório *North American Pulse of Internal Audit* de 2023

Pesquisa *Pulse of Internal Audit* do IIA, de 20 de outubro a 2 de dezembro de 2022. Q25: Quando está realizando trabalhos de auditoria em geral, quais das seguintes áreas você costuma incluir em suas considerações? (Escolha todas as aplicáveis.) n = 555.

De fato, os dados do próximo relatório North American Pulse of Internal Audit de 2023 mostram que a fraude é a consideração mais citada nas auditorias internas. A pesquisa anual com CAEs norte-americanos pediu a mais de 500 participantes que indicassem quais áreas incluem como parte de suas auditorias em geral. "As respostas indicam que os auditores geralmente adotam uma abordagem holística e consideram uma ampla gama de questões, incluindo cibersegurança, terceiros e governança", de acordo com o relatório, que será lançado em março na Conferência GAM de 2023. No geral, 89% dos CAEs disseram que incluem considerações de fraude em cada auditoria em geral, que foi a categoria de risco mais citada, com as considerações de TI em segundo lugar com 80%.

[6] Declaração de Posicionamento do IIA, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[7] *Premier Global Research* de 2022, *Internal Audit: A Global View*, Internal Audit Foundation, 2022.

De acordo com a Declaração de Posicionamento do IIA *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*,[8] a auditoria interna deve ter o conhecimento necessário sobre fraude para ser capaz de:

- Identificar alertas vermelhos que possam indicar que uma fraude foi cometida.
- Compreender as características da fraude e as técnicas utilizadas para cometê-la, bem como os tipos de esquemas e cenários de fraude.
- Ser capaz de decidir se uma ação adicional é necessária ou se uma investigação deve ser recomendada.
- Avaliar a eficácia dos controles para prevenir ou detectar fraudes e identificar oportunidades de melhoria.

[8] Declaração de Posicionamento do IIA, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

O Papel do Examinador de Fraude

Investigando engano

A investigação qualificada de fraude é fundamental

O examinador de fraude participa e apoia os programas gerais de exame de fraude da organização. Ele faz isso em parte conduzindo investigações de fraude que "buscam obter fatos e evidências para ajudar a estabelecer o que aconteceu, identificar a parte responsável e fornecer recomendações quando aplicável".[9] Uma das questões que um examinador considera ao iniciar uma investigação é a *predicação*, que significa que a totalidade das circunstâncias deve fazer parecer razoável para um profissional bem treinado que a fraude ocorreu.

Os passos seguidos por um examinador de fraude em uma investigação podem incluir a obtenção de evidências, reportar o que for encontrado, testemunhar sobre essas descobertas conforme necessário e auxiliar na detecção e prevenção de fraudes. Dois propósitos comuns para um exame de fraude são uma investigação de uma possível fraude ou alegação de fraude, e uma revisão das políticas e controles antifraude de uma organização. Objetivos mais específicos por trás de um exame de fraude podem incluir:

- Detectar conduta imprópria que esteja ou possa estar associada a fraude, bem como determinar quem é responsável por qualquer comportamento impróprio.
- Determinar as perdas ou responsabilidades reais ou potenciais da fraude.
- Demonstrar o compromisso da organização em identificar e mitigar fraudes.
- Ajudar a facilitar a recuperação de perdas.
- Prevenir fraudes futuras e perdas ou responsabilidades relacionadas.
- Abordar as consequências além das perdas financeiras.
- Identificar e fortalecer pontos fracos nos controles internos.
- Quando exigido em alguns casos, cumprir com estatutos, regulamentos, contratos ou deveres de direito comum.[10]

[9] "Planning and Conducting a Fraud Examination," *Fraud Examiners Manual: 2022 Edition*, ACFE.
[10] ibid

Comparando abordagens

Esta tabela oferece uma visão geral de algumas diferenças importantes entre os papéis, abordagens e metas dos auditores internos e CFEs.

Características	Auditoria Interna	Exame de Fraude
Intenção	Os procedimentos de auditoria interna podem revelar fraudes, mas não garantem que serão detectadas. Por exemplo, os auditores podem encontrar uma transação ou situação suspeita em uma revisão e ela pode ser identificada como fraude. No entanto, encontrar fraudes será apenas um aspecto de um exame mais amplo de controles e procedimentos dentro da área sob auditoria.	Um exame de fraude está diretamente focado em descobrir fraudes e considerar ações ou atividades antifraude.
Ocorrência	As auditorias são normalmente recorrentes regularmente, embora as auditorias *"pop-up"* possam ser usadas para abordar uma situação única ou questões em uma área.	Exames de fraude são normalmente conduzidos apenas se houver predicação suficiente, embora possam ocorrer sem qualquer gatilho específico, como parte de um programa de gerenciamento de riscos ou avaliação do risco de fraude. No entanto, a maioria é conduzida em resposta a denúncias ou alegações. A pesquisa da ACFE constatou que 43% das fraudes foram detectadas por causa de denúncias, o que foi quase três vezes o número do próximo método mais comum para encontrar fraudes. Mais da metade de todas as denúncias de fraude vieram de funcionários.
Antagônica ou não?	As auditorias internas são de natureza não antagônica. O objetivo dos auditores é oferecer insights e informações que os líderes e membros da equipe possam usar para melhorar controles ou outros processos, por exemplo.	Os exames de fraude são inerentemente antagônicos. Parte do objetivo é colocar a culpa em quem está cometendo a fraude.
Normas	Os auditores internos seguem as *Normas Internacionais para a Prática Profissional de Auditoria Interna*, estabelecidas pelo *Institute of Internal Auditors* (IIA).	CFEs seguem o *Code of Professional Standards* da ACFE. CFEs podem usar uma ferramenta de avaliação de risco de fraude da ACFE em seus exames.

Colaborando no Trabalho

Respeito Mútuo e Responsabilidades

Trabalhando na batalha contra a fraude

Há inúmeras oportunidades para colaboração benéfica entre auditores e examinadores de fraude. Eles podem consultar uns aos outros sobre:

- Início de uma investigação de fraude
- Planejamento anual de exames de auditoria e de fraude
- Avaliações de riscos
- Avaliação e análise de controles e de programas antifraude
- Transmissão das constatações de auditoria com implicações de fraude
- Remediação de deficiências de controle.

Muitas organizações têm regras que regem os protocolos quando a auditoria interna passa uma constatação de fraude para uma equipe de exame de fraude externa ou interna. A equipe de auditoria interna anota a constatação de fraude e faz um relatório conjunto com o examinador de fraude no fim da revisão.

Além disso, a auditoria interna pode auditar o departamento antifraude de uma organização, para garantir que seus próprios controles sejam adequados. Uma equipe antifraude pode reportar às equipes jurídica ou de gerenciamento de riscos corporativos, entre outras áreas, incluindo a auditoria interna. Caso uma equipe de fraude reporte à auditoria interna, qualquer auditoria desse departamento deveria ser terceirizada, para garantir a objetividade.

Estudo de caso ilustra a colaboração no trabalho

O estudo de caso a seguir demonstra como as duas equipes podem trabalhar juntas. É baseado em uma discussão de Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB, diretora de desenvolvimento de produtos do IIA, em um recente webinário do IIA e da ACFE, *Fostering Collaboration: The Auditor and the Fraud Examiner.*

Normalmente, a auditoria interna descobre um padrão que se assemelha a uma fraude e alerta os examinadores de fraude. No caso apresentado por Flanders, uma auditoria interna incluía uma revisão de empréstimos para automóveis. Uma das medidas tomadas por sua equipe foi avaliar as contas inadimplentes. Em um grupo de 40 contas, cinco delas se destacaram. O sistema foi configurado para sinalizar empréstimos inadimplentes que deveriam ser acompanhados, mas, por alguns motivos, esses cinco não foram sinalizados. Além disso, todos foram configurados com características bastante inusitadas: taxa de juros de 0%, prazo de 72 meses e sem pagamento mínimo.

Quando Flanders investigou, ela descobriu que o ID do usuário associado aos empréstimos pertencia a um representante de atendimento ao cliente, o que não fazia sentido. Pessoas nessa função geralmente não aprovavam empréstimos. Então, ela revisou os arquivos de log relacionados aos empréstimos e descobriu que, cerca de uma hora antes de cada um ser enviado e aprovado, o titular do ID do usuário recebia acesso adicional ao sistema. Esse acesso era removido cerca de uma hora depois que os empréstimos eram aprovados e ativados. Considerando os termos incomuns do empréstimo, o envolvimento do representante de atendimento ao cliente e as mudanças no acesso ao sistema, a equipe de auditoria sabia que era hora de entregar o caso ao departamento de fraudes da empresa.

Dependendo das políticas e procedimentos da organização, os passos que o departamento de fraude pode executar nesse caso, quando alertado sobre uma atividade suspeita, incluem:

- Corroborar as informações recebidas dos auditores.
- Examinar todo o escopo das atividades relacionadas a essas contas.
- Determinar se a criação dessas cinco contas foi uma ação única ou parte de um possível esquema contínuo.
- Identificar quaisquer outros comparsas.
- Considerar se outras filiais ou escritórios estão envolvidos e o escopo geral da fraude.

Neste ponto, os examinadores de fraude também podem considerar se e como a fraude deve ser interrompida. Se forem necessárias mais evidências ou informações, pode-se decidir que a fraude deve continuar, pelo menos temporariamente. Essa é uma determinação complicada, que dependerá do quanto a empresa já perdeu, quanto poderia perder potencialmente se a fraude continuar, e do apetite a risco da organização, de acordo com Mason Wilder, CFE, gerente de pesquisa da ACFE, que também participou do webinário. Nesse caso, os passos a serem executados antes de interromper a fraude podem incluir entrevistar o representante de atendimento ao cliente, para obter mais informações e identificar o escopo da fraude e, potencialmente, descobrir fraudes adicionais ou planos para tal.

Depois de reunir e analisar as evidências, os examinadores de fraude reportariam suas descobertas — oralmente ou por escrito — às pessoas apropriadas na organização. Isso pode incluir a gestão, o conselho ou o comitê de auditoria. "Um relatório de exame de fraude é uma narração das atividades específicas do examinador de fraude, descobertas e, se apropriado, recomendações", de acordo com o *Fraud Examiners Manual* da ACFE. A gestão da organização pode usar o relatório para determinar os próximas passos apropriados.

Se os examinadores de fraude revisarem a situação e não encontrarem fraude real, eles podem devolver o caso, se determinarem que o alerta vermelho original surgiu por uma deficiência nos controles de gerenciamento do risco de fraude. A auditoria interna poderia, então, incluir essa deficiência em seu relatório.

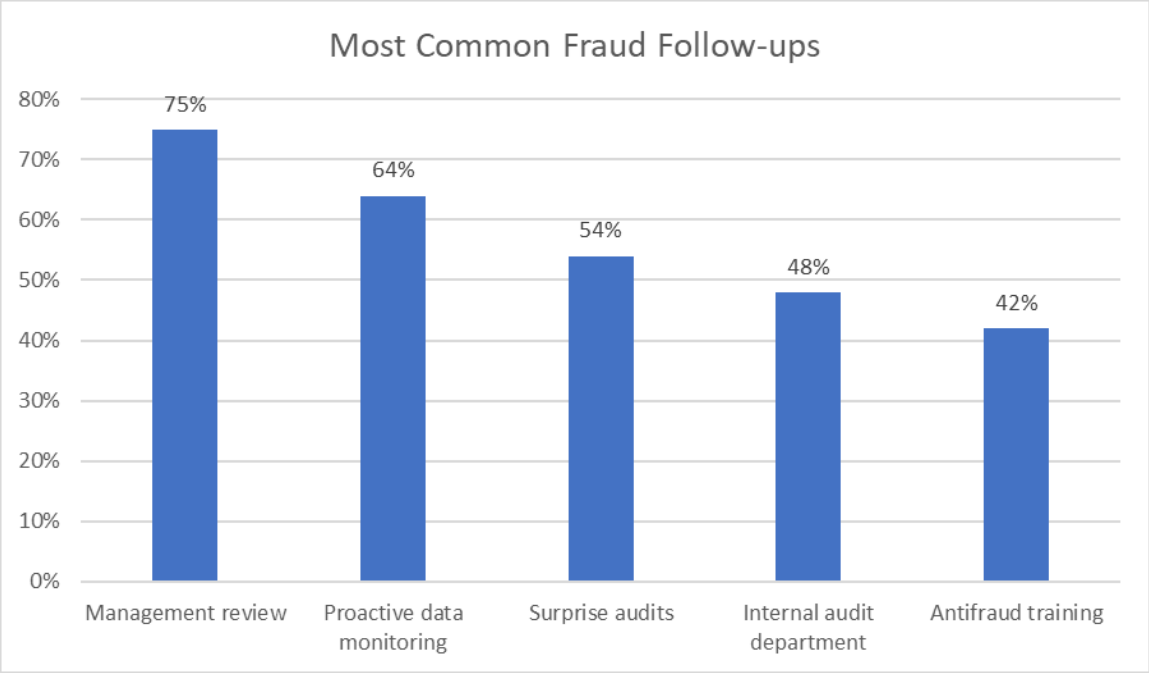
Combinando forças

Aqueles preocupados com a fraude devem se lembrar de que a mitigação é importante. O relatório da pesquisa da ACFE observou que medidas proativas para encontrar fraudes podem levar à detecção precoce e perdas menores, enquanto esforços reativos permitem que os esquemas durem mais tempo e aumentem o impacto financeiro sobre a vítima.

No entanto, as organizações não podem identificar ou eliminar todos os riscos de fraude. Elas enfrentam vários tipos de fraude, uma variedade de motivações por trás delas e uma ampla gama de malfeitores. No entanto, quanto mais informadas estiverem as pessoas em todos os níveis — gestão, conselho e equipe —, melhores elas serão na implantação de esforços razoáveis de mitigação e na identificação de fraudes ou dos sinais de alerta que possam indicar sua existência. Combinando suas habilidades e experiências únicas, os auditores internos e os examinadores de fraude podem dar uma forte contribuição aos esforços gerais da organização. As organizações podem usar seu trabalho para tomar decisões mais informadas sobre abordagens de gerenciamento do risco de fraude.

Passos para prevenir a recorrência

Um total de 81% das organizações na pesquisa da ACFE fez modificações em seus controles antifraude após uma fraude. O gráfico abaixo mostra as mudanças mais comuns nos controles que as organizações implantaram ou modificaram. Outros controles antifraude recomendados pela ACFE incluem o monitoramento automatizado de transações/dados, vigilância e reconciliação de contas.



Fonte: *Occupational Fraud 2022: A Report to the Nations*, *Association of Certified Fraud Examiners*.

Conclusão

O papel da auditoria interna como prestador de avaliação da terceira linha sobre governança, risco e controle interno requer estruturas, processos e práticas que promovam uma avaliação objetiva e independente. Mas, conforme observado no Modelo das Três Linhas do IIA, independência não significa isolamento.

“Deve haver interação regular entre a auditoria interna e a gestão, para garantir que o trabalho da auditoria interna seja relevante e alinhado às necessidades estratégicas e operacionais da organização. Por meio de todas as suas atividades, a auditoria interna constrói seu conhecimento e compreensão da organização, o que contribui para a avaliação e assessoria que ela oferece como conselheira confiável e parceira estratégica”, de acordo com o Modelo.

Este é claramente o caso quando a auditoria interna e os examinadores de fraude certificados encontram consenso como aliados na batalha contra a fraude.

Parte 3

A Ressaca: Fraude na Era Pós-COVID

Sobre os Especialistas

David Dominguez, CIA, CRMA, CPA, CFE

David é diretor de auditoria e conformidade da Itafos em Houston. Em sua carreira, David trabalhou com empresas multinacionais em várias indústrias, para estabelecer, dirigir e transformar as funções de auditoria interna corporativas e regionais. Liderou e executou projetos financeiros, operacionais e de avaliação e assessoria de TI na América do Norte, América Latina, Europa e Ásia. Também gerenciou e participou de várias investigações multijurisdicionais, iniciativas de análise de dados e uma ampla variedade de auditorias internacionais de acionistas, joint ventures e fornecedores. Suas áreas de especialização incluem governança corporativa e organizacional, gerenciamento de riscos corporativos, gerenciamento do risco de fraude, a Lei Sarbanes-Oxley de 2002 e programas de ética e conformidade.

Introdução

Durante a maior parte de dois anos, o COVID-19 causou disrupção em todos os setores, desde a forma como as pessoas trabalhavam, onde trabalhavam, como suas organizações lidavam com fornecedores e questões da cadeia de suprimentos, e como lidavam com preocupações significativas, como manter controles internos e detecção e prevenção de fraudes.

Hoje, o mundo respira com mais facilidade, conforme o pior da pandemia desaparece lentamente na história, mas, mesmo assim, não se deve presumir que os riscos associados ao COVID-19 não sejam mais uma preocupação. Na verdade, as organizações que fazem essa suposição podem estar cometendo um grave erro. *Este* Brief de Conhecimento Global, o terceiro de uma série de três partes sobre fraude do *The Institute of Internal Auditors* (IIA), examina vários fatores de fraude relacionados à pandemia identificados no *Report to the Nations* da ACFE de 2022, como podem impactar as organizações e o papel da auditoria interna nos esforços organizacionais para mitigar esses fatores de risco de fraude.

Fraude e Riscos de Fraude Persistem

Mudanças relacionadas à pandemia continuam sendo uma preocupação

Novas fraudes inspiradas pelo COVID surgirão

No mais recente *Report to the Nations* sobre fraude ocupacional, a *Association of Certified Fraud Examiners* (ACFE) constatou que a duração mediana das fraudes – ou seja, o tempo típico entre o início de uma fraude e o momento em que é detectada – era de 12 meses.[11] Isso significa que as organizações continuam enfrentando fraudes relacionadas à pandemia que ainda não foram descobertas.

Há muitas razões pelas quais as mudanças relacionadas à pandemia continuam a impactar o risco de fraude. Por exemplo, a adoção do trabalho remoto era para ser temporária, mas se transformou em procedimento operacional padrão em muitas empresas. O trabalho remoto, muitas vezes, trouxe consigo mudanças significativas – e, em alguns casos, afrouxamento – nas práticas e procedimentos destinados a identificar ou mitigar fraudes. Como resultado, os riscos associados continuam representando ameaças para as empresas, mesmo conforme as disrupções relacionadas à pandemia diminuíram.

A auditoria interna desempenhou e continuará desempenhando um papel fundamental no tratamento dos riscos prolongados de fraude relacionados à pandemia. Em um estudo com membros do IIA do mundo todo, conduzido pela *Internal Audit Foundation* (IAF) e Kroll, muitos participantes de mesas redondas relacionadas sentiram que a pandemia "coloca a auditoria interna mais no comando, quando se trata do gerenciamento do risco de fraude."[12] Isso inclui envolvimento adicional em considerações estratégicas de desafios operacionais, prestação de avaliação contínua e maior colaboração entre as funções de negócios — tudo isso mantendo a independência do auditor.

[11] *Occupational Fraud 2022: A Report to the Nations*, ACFE.
[12] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, Internal Audit Foundation e Kroll, março de 2022.

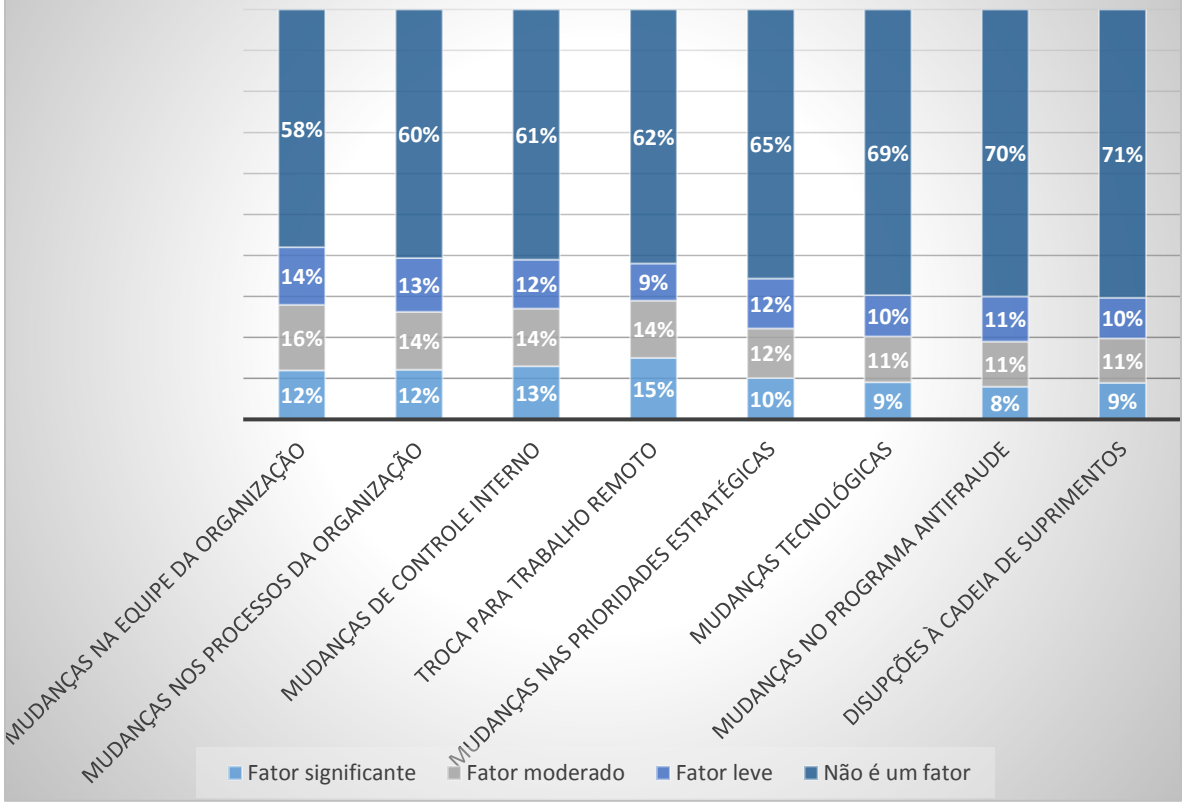
Principais Riscos de Fraude da Pandemia

Mudanças na equipe e trabalho remoto são as maiores preocupações

Mais da metade vê fatores pandêmicos contribuindo para a fraude

Ao preparar seu relatório sobre fraude ocupacional, a ACFE constatou que 52% dos entrevistados reportaram que, em incidentes de fraude que investigaram, pelo menos uma das diversas questões relativas à pandemia contribuiu para a fraude. Entre elas, mudanças organizacionais relativas à pandemia foram as mais comuns. Um total de 42% dos entrevistados disse que as mudanças na equipe foram fatores significativos, moderados ou leves que contribuíram para a fraude ocupacional. A troca para o trabalho remoto foi o fator mais citado como significativo (15%), seguido pelos controles internos (13%) (ver Figura 1).

Figura 1: O quanto os fatores relativos à pandemia contribuíram para fraudes ocupacionais?



Fonte: *Occupational Fraud 2022: A report to the Nations,* ACFE.

Um exame mais profundo de algumas das principais questões relativas à pandemia identificadas no relatório da ACFE mostra que os impactos podem ser frequentemente complexos e sutis.

Mudanças na equipe apresentam diversos riscos de fraude

A pandemia forçou muitas organizações a encontrar soluções alternativas ou atalhos para lidar com as tantas disrupções que enfrentavam, incluindo mudar ou expandir as responsabilidades dos trabalhadores ou trazer novas pessoas que tinham tempo limitado para se acostumar com seus trabalhos. Além disso, cortes temporários ou licenças resultantes da incerteza econômica relativa à pandemia muitas vezes se tornaram permanentes, observou David Dominquez, diretor de auditoria e conformidade da Itafos, uma empresa de fosfato e fertilizantes especiais. "Definitivamente, aumentou o risco a partir de diversos ângulos", disse ele.

Dados os muitos ajustes e acomodações nas práticas e protocolos de trabalho que a pandemia pode ter criado – e a potencial curva de aprendizado para quem assume novas tarefas –, as organizações devem considerar quais tipos de impactos não intencionais essas mudanças podem ter tido. Aqui estão algumas áreas a serem consideradas:

Cultura

Há uma série de razões para reavaliar e, talvez, reafirmar a cultura e os valores corporativos após a pandemia. "Fazer dar certo" foi uma virtude durante a pandemia, mas isso pode significar que algumas práticas e atitudes éticas importantes foram esquecidas. Os novos funcionários também podem nunca ter passado por uma introdução adequada aos valores éticos da empresa. Se esse for o caso, as organizações fariam bem em lembrar os funcionários de suas expectativas sobre comportamentos éticos.

"Uma abordagem proativa à cultura pode impedir vários tipos de má conduta e promover comportamentos que podem aumentar o moral e a produtividade", disse a ACFE em seu relatório. "A cultura tem uma capacidade poderosa de afetar a forma como as pessoas fazem seu trabalho; como são tomadas as decisões sobre qualidade, conformidade e outras preocupações críticas; e como a organização é percebida interna e externamente."[13]

Considerações de recursos humanos

A escassez de mão de obra e as mudanças nas políticas de trabalho híbrido e remoto derrubaram algumas práticas de recursos humanos de longa data, como canais de denúncias anônimas.

Uma importante ferramenta relacionada ao RH na prevenção de fraudes é o canal de denúncias anônimas. De acordo com o relatório da ACFE, 42% das fraudes foram detectadas por denúncias, mais que o triplo da porcentagem do próximo método mais comum.

A auditoria interna pode apoiar esse processo, examinando se ele está funcionando conforme o esperado. O primeiro passo pode ser determinar o quão bem esses canais são monitorados e se as reclamações são acompanhadas e rastreadas, disse Dominquez. Ele recomenda fazer perguntas aos monitores do canal de denúncias, como:

- **Como as pessoas acessam o canal de denúncias?** As opções incluem deixar informações em uma caixa de depósito no escritório, ligar para um número de linha direta ou reportar reclamações online. Lembre-se de que usar uma caixa de depósito – e cartazes promovendo a linha direta – não funcionará para trabalhadores remotos.
- **O canal pode ser disponibilizado em diferentes idiomas, se apropriado?**
- **Quão bem o esforço está sendo rastreado?** Dominquez observou que algumas empresas se parabenizam pelo baixo número de reclamações. Isso pode ser um reflexo preciso de uma organização bem administrada, mas também pode indicar que algumas ligações de denúncias não são atendidas ou que as reclamações são raramente investigadas.

A auditoria interna pode revisar o processo de resposta a reclamações, para garantir o tempo adequado desde a entrada até a resolução e se é bem fundamentada a decisão de investigar ou não. Às vezes, as organizações deixam de receber

[13] *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, *Anti-Fraud Collaboration*, março de 2020.

denúncias válidas de fraude por medo de retaliação após a denúncia. A auditoria interna pode verificar se o manual corporativo ou código de conduta proíbe explicitamente a retaliação. Indo além, a auditoria interna também pode ajudar a empresa a rastrear se os denunciantes são menos propensos a obter uma promoção ou mais propensos a obter uma avaliação de desempenho ruim, observou Dominquez. Mesmo quando uma reclamação for infundada, as empresas podem encontrar no processo de resposta políticas que precisam ser atualizadas ou esclarecidas, disse.

Outras precauções/controles valiosos que as organizações devem manter ou implantar incluem:

- Verificações de antecedentes, para identificar o histórico anterior de crédito ou outros problemas financeiros, ou um histórico de penhoras salariais, ônus ou julgamentos que possam estar associados a peculato.
- Verificação de credenciais.

A ACFE reportou que 50% dos fraudadores exibiram pelo menos um alerta vermelho relacionado a RH antes ou durante o incidente de fraude. Em termos de pistas comportamentais, viver além de seus meios tem sido o sinal de alerta mais comum em todos os estudos da ACFE desde 2008. Foi identificado em 39% dos casos, bem à frente do segundo fator mais comum, dificuldades financeiras, com 25%.

Incerteza empregatícia

A ACFE identificou vários exemplos de incerteza empregatícia que podem contribuir para a fraude, e condições econômicas desafiadoras podem aumentar essa insegurança. Os alertas vermelhos específicos incluem:

- Medo de perder o emprego.
- Negação de aumento ou promoção.
- Corte nos benefícios.
- Corte no pagamento.
- Corte involuntário nas horas.
- Rebaixamento.

Embora o clima econômico tenha se estabilizado desde os piores dias da pandemia, os desafios permanecem no clima de negócios global. Não surpreendentemente, o impacto das questões relacionadas à incerteza no trabalho permaneceu forte em 2022, de acordo com a ACFE. É lógico que algumas dessas incertezas ainda podem ser um fator na ocorrência de má conduta dos funcionários.

Esses alertas vermelhos aplicam-se a funcionários em geral, mas há alguns outros que se aplicam especificamente a executivos da alta administração:

- **Bullying ou intimidação.** 23% para proprietários/executivos; 8% para não proprietários/executivos.
- **Questões de controle.** 18% para proprietários/executivos; 12% para não proprietários/executivos.
- **Comportamento de "trapaceiro".** 17% para proprietários/executivos; 9% para não proprietários/executivos.
- **Pressão excessiva de dentro da organização.** 13% para proprietários/executivos; 6% para não proprietários/executivos.
- **Problemas legais anteriores.** 11% para proprietários/executivos; 3% para não proprietários/executivos.

Mudanças de controle interno relacionadas ao COVID devem ser revisitadas

Os controles internos são procedimentos adotados para garantir que as ações e decisões em toda a organização estejam alinhadas com suas políticas, requisitos de reporte e mandatos de conformidade. Os controles antifraude podem reduzir as perdas por fraude e facilitar a detecção de fraudes mais rapidamente. No estudo da ACFE, quase metade das perdas por fraude pode ser atribuída a dois fatores: falta de controles internos (29%) e capacidade de contornar os controles existentes (20%). Implantar e fortalecer os controles internos pode claramente fornecer um benefício positivo significativo para as organizações. A auditoria interna tem um papel importante a desempenhar, ao reportar os controles internos e recomendar melhorias para eles. De fato, a pesquisa da ACFE constatou que a perda mediana por fraude era 50% maior (US$ 150.000 x US$ 100.000) quando não havia departamento de auditoria interna.

Os auditores internos que responderam à pesquisa da IAF/Kroll acreditam que "o framework de controle interno foi enfraquecido devido aos desafios do trabalho remoto e, em muitos casos, à redução de equipe por motivo de doença, licenças e cortes".[14]

Novas pessoas que ingressam em organizações em tempos de crise podem não ter recebido treinamento ou transferência de conhecimento suficiente, ou podem ter aprendido apenas protocolos de emergência, que não incluíam processos e controles de longa data, disse Dominquez. "Os controles foram diluídos, ou talvez apenas tenham passado despercebidos", disse ele. Ao longo do caminho, tais atalhos podem se tornar — e continuar sendo — procedimento operacional padrão, mesmo que tenham sido feitos para uso apenas durante um período específico ou em uma situação particular.

Essa preocupação tem levado a mudanças positivas em muitas organizações. Por exemplo, cerca de três quartos dos membros do comitê de auditoria que responderam a uma pesquisa conjunta do *Center for Board Effectiveness* da Deloitte e do *Center for Audit Quality* disseram ter atualizado seus controles internos no ano passado, devido ao ambiente de trabalho remoto.[15]

As deficiências nos controles internos podem contribuir para a fraude, ao criar ou promover um ambiente em que seja mais fácil negligenciar ou contornar medidas robustas antifraude. Por exemplo, durante a pandemia, a segregação de funções — uma medida antifraude comum e eficaz — pode ter sido deixada de lado, porque era mais difícil de realizar com trabalhadores espalhados por locais diferentes, ou devido a cortes ou escassez de pessoal. Esse é o tipo de controle interno que uma empresa deve revisar agora, para garantir que tenha sido restabelecido e que esteja funcionando de forma eficaz.

A auditoria interna pode ajudar as organizações a lidar com esses riscos, garantindo que protocolos e processos vitais estejam em vigor. Usando a tecnologia de mapeamento de processos, podem acompanhar os processos durante um período recente — seis meses ou um ano — e identificar variações em relação às diretrizes adequadas ou às melhores práticas. "Você pode ver desvios de procedimentos ou políticas padrão e identificar quais processos precisam ser atualizados ou aplicados", disse Dominquez.

Outras áreas a serem revisadas incluem controles internos relacionados a aquisições, emissão de cheques, conciliação bancária, reembolsos de despesas ou qualquer área envolvida em considerações financeiras.

O trabalho remoto continua sendo um fator crítico de fraude

A troca dramática para o trabalho remoto – que fechou escritórios e permitiu que os trabalhadores realizassem seus trabalhos em casa – foi provavelmente a mudança mais significativa para a maioria das organizações durante a pandemia. Consequentemente, essa nova abordagem foi o fator mais citado como tendo contribuído significativamente para a fraude

[14] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, Internal Audit Foundation e Kroll, março de 2022.
[15] *Audit Committee Practices Report: Common Threads Across Audit Committees*, *Center for Board Effectiveness* da Deloitte e *Center for Audit Quality*, 25 de janeiro de 2022.

no relatório da ACFE. Em circunstâncias normais, uma empresa pode passar meses considerando o impacto estratégico de tal movimento, mas isso era essencialmente impossível em meio à incerteza e à urgência das primeiras semanas da pandemia. No mínimo, trabalhar sozinho e fora do campo de visão de colegas e supervisores pode simplesmente facilitar a perpetração de uma variedade de fraudes. Aqueles que estão fazendo ou fizeram uma mudança permanente para o trabalho remoto ou híbrido devem se envolver no planejamento de gestão de mudanças, "para descobrir as falhas que podem ter consequências catastróficas se não forem abordadas", de acordo com o ACFE.[16]

Ao longo desse processo, há diversas falhas potenciais nas quais a auditoria interna pode se concentrar. Por exemplo, as dificuldades de administrar eficazmente as pessoas em um ambiente remoto fragmentado e seu impacto sobre a cultura foram citados como áreas principais a serem abordadas, de acordo com o relatório da IAF/Kroll.[17] O comportamento ético geralmente é algo que é aprendido e reforçado por meio de interações com outros trabalhadores que o exemplificam no trabalho. O acesso a colegas mais experientes pode ajudar os funcionários a entender como agir em circunstâncias confusas ou suspeitas, como quando outro funcionário parece estar agindo de forma inadequada ou ilegal.

Entre os tipos de fraude especificamente associados ao trabalho remoto estão:

- **Roubo de tempo ou alegações imprecisas sobre as horas trabalhadas.** Isso pode ser mais fácil de fazer quando alguém não está sob supervisão direta.
- **Roubo de dados, ou uso indevido ou compartilhamento de informações confidenciais ou sensíveis.** Isso pode ser feito por quem pode obter acesso aos dispositivos de um funcionário, ou por funcionários que se sentem mais à vontade para fazer uso indevido de dados quando estão fora do escritório.[18]

Uma preocupação relacionada é que funcionários remotos assumam trabalhos secundários. Por exemplo, um funcionário pode prestar consultoria ou tarefas temporárias para outra empresa durante o horário em que deveria trabalhar para seu empregador principal, disse Dominquez. Isso certamente é roubo de tempo, mas o uso indevido de recursos da empresa, como laptops ou telefones, também pode expor a empresa a problemas de cibersegurança. O trabalho paralelo também pode ser um conflito de interesses, se o funcionário estiver trabalhando para um concorrente, especialmente se compartilhar informações que sejam benéficas para a concorrência. A auditoria interna pode ajudar a resolver esse problema, questionando o tipo de treinamento que os funcionários recebem e se o manual e as políticas do funcionário foram atualizados para os novos ambientes de trabalho, disse Dominquez.

Mudanças tecnológicas criam uma dicotomia de fraude

A tecnologia pode permitir que as organizações implantem procedimentos eficazes em áreas como controles internos e trabalho remoto. As organizações já estavam fazendo melhorias e investimentos em tecnologia para lidar com as preocupações de cibersegurança, e a pandemia estimulou as empresas a acelerar e fortalecer seus sistemas. Muitas funções de auditoria interna foram incluídas na atualização tecnológica. De fato, 29% dos auditores internos acrescentaram a análise de dados como ferramenta para identificar fraudes e corrupção desde o início da pandemia.[19]

Ao mesmo tempo, o uso indevido ou a negligência de ferramentas tecnológicas pode facilitar o sucesso de esquemas de fraude. Conforme observado, o roubo de dados é uma das preocupações associadas ao trabalho remoto. Possíveis soluções para riscos de roubo de dados, de acordo com a ACFE, incluem exigir que os funcionários protejam sua rede doméstica — e não a compartilhem com outros membros da família. O uso de VPNs e de senhas e configurações mais fortes e complexas para proteger os computadores domésticos também é fundamental. Outras opções incluem autenticação multifator e treinamento anual para funcionários sobre segurança e privacidade de dados. As organizações também devem

[16] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 de janeiro de 2023.
[17] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, Internal Audit Foundation e Kroll, março de 2022.
[18] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 de janeiro de 2023.
[19] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, Internal Audit Foundation e Kroll, março de 2022.

desenvolver políticas sobre o uso aceitável de dispositivos eletrônicos, redes sociais e dados da empresa, bem como exigir que os funcionários leiam e reconheçam que entendem as políticas.

As organizações que trabalham em um ambiente remoto ou híbrido também precisam garantir que os funcionários atualizem patches de software e de segurança em seus dispositivos domésticos, além de educar os funcionários sobre as melhores formas de evitar phishing e outras ameaças de hackers.[20] Obviamente, as empresas que se esforçaram para acompanhar o impacto da pandemia devem revisar suas próprias medidas de cibersegurança, para garantir que permaneçam atualizadas.

Para ajudar a resolver essas preocupações, Dominquez recomendou que a auditoria interna investigue quais protocolos de segurança estão em vigor, quais ferramentas de prevenção contra perda de dados a organização está usando, se requer autenticação multifator e VPNs, e se as contas são desativadas tempestivamente quando os funcionários saem.

"Demissão Silenciosa" afeta os esforços de conformidade e ética

A "demissão silenciosa" (em inglês, *"quiet quitting")* refere-se a uma prática em que os trabalhadores fazem apenas o mínimo de suas exigências de trabalho. De acordo com uma estimativa da Gallup, esses trabalhadores representam pelo menos 50% da força de trabalho dos EUA. O nível de trabalhadores engajados estava em 32%, mas aqueles ativamente desengajados chegavam a 18%. A Gallup observa que isso é especialmente problemático em um momento em que muitos trabalhos são colaborativos, ou quando pode ser necessário um passo extra para atender às necessidades do cliente. E embora a tendência de demissão silenciosa tenha recebido muita atenção, os empregadores devem estar cientes de que demissões barulhentas – ou pessoas que se expressam ativamente e talvez espalhem sua insatisfação – ainda existem.[21]

Essa tendência pode ser uma má notícia para produtividade, eficiência e retenção. Ao mesmo tempo, pode ter um efeito negativo no gerenciamento de riscos. "As pessoas não estão prestando tanta atenção ao que deveriam fazer", disse Dominquez. E, como observa o *Corporate Compliance Insights*, um programa bem-sucedido de conformidade e ética requer a participação e o apoio de todos em uma organização. "Quando você combina uma visão relativamente negativa do trabalho com uma abordagem de 'mínimo trabalho viável', aqueles esforços extras com os quais os profissionais de conformidade e ética contam para garantir que as pessoas levantem questões geralmente desaparecem", observou.[22]

Isso certamente também é verdade para um programa de gerenciamento do risco de fraude. Os funcionários podem estar carimbando aprovações e transações ou ignorando anomalias, ou podem escalar uma anomalia apenas para descobrir que seu gerente do nível seguinte a ignorou para ter uma demissão silenciosa.

A auditoria interna pode examinar pesquisas de satisfação do funcionário, taxas de rotatividade e entrevistas de desligamento para ter uma noção dos problemas de engajamento do funcionário. As tendências recentes podem ser comparadas com a atividade antes da pandemia, para entender o impacto que ela pode ter tido, disse Dominquez.

[20] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 de janeiro de 2023.
[21] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, 6 de setembro de 2022.
[22] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, 14 de setembro de 2022.

Conclusão

A que conclusão chegamos? De acordo com a ACFE, as organizações perdem cerca de 5% da receita por fraude todos os anos, com uma perda mediana de US$ 117.000 e uma perda média de US$ 1.783.000. Normalmente, as perdas em esquemas de fraude podem chegar a US$ 8.300 por mês. Essas são considerações sérias para qualquer organização.

Durante e desde o pior da pandemia, as organizações recorreram aos auditores internos para ajudar os tomadores de decisões estratégicas a reavaliar e melhorar os processos operacionais. Essa prática deve continuar, principalmente na avaliação dos controles internos antifraude. O mundo pode ter emergido da pandemia, mas não necessariamente se livrou das ameaças de fraude relacionadas à pandemia.

Desde o início da pandemia, houve uma apreciação ainda maior pelas contribuições que a auditoria interna pode fazer para mitigar ou impedir fraudes. No passado, a auditoria interna costumava ser chamada depois que um incidente de fraude já havia ocorrido. Isso está mudando; as organizações agora estão menos propensas a esperar para detectar a fraude, e esperam resolvê-la antes que muitos danos sejam causados. Para ajudar a conseguir isso, estão envolvendo os auditores internos em conversas de prevenção, em outras palavras, pedindo-lhes que considerem os controles antifraude antes que a fraude aconteça, disse Dominquez. A auditoria interna também está facilitando discussões sobre avaliação do risco de fraude e frameworks de avaliação do risco de fraude, considerando a frequência e a eficácia dessas avaliações e testes de controle, e observando quaisquer mudanças no perfil de risco contínuo da empresa. “Em vez de esperar para detectar fraudes, os auditores internos estão migrando para o lado preventivo”, disse Dominquez.

Sobre o The IIA

The Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos que atende a mais de 230.000 membros globais, tendo concedido mais de 185.000 certificações *Certified Internal Auditor* (CIA) no mundo todo. Fundado em 1941, o The IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, visite theiia.org.

Isenção de Responsabilidade

The IIA publica este documento para fins informativos e educacionais. Este material não se destina a fornecer respostas definitivas a circunstâncias individuais específicas e, como tal, destina-se apenas a ser usado como guia. The IIA recomenda buscar assessoria especializada independente relacionada diretamente a qualquer situação específica. The IIA não aceita qualquer responsabilidade por qualquer pessoa que confie exclusivamente neste material.

Copyright

Abril de 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101