IPPF

International Professional Practices Framework

Orientação Suplementar

Guia Prático

Planejamento do Trabalho

Avaliando Riscos de Fraude

The Institute of Internal Auditors | Global

Tabela de Conteúdos

Sumário Executivo 3
Introdução 4
Entendendo a Fraude 5
Coletando Informações 6
Avaliações e Investigações Anteriores 7
Mecanismos de Reporte Formais e Entrevistas 7
Revisão Preliminar do Ambiente de Controle 8
Pesquisa Externa e Especialistas 9
Brainstorming de Cenários de Fraude 10
Avaliando Riscos de Fraude 11
Identificando Controles 14
Anexo A. Normas e Orientações do The IIA 15
Anexo B. Glossário 16
Anexo C. Exemplos de Atos Fraudulentos 17
Anexo D. Possíveis Palavras de Alerta a Considerar 18
Anexo E. Estudo de Caso: Trabalho de Avaliação de Despesas em Dinheiro 19
Agradecimentos 22

Sumário Executivo

A fraude pode atrapalhar as operações, apresentar riscos de conformidade, macular a reputação de uma organização e custar à organização e às suas partes interessadas quantias substanciais de dinheiro. Embora a administração, com supervisão do conselho, tenha a responsabilidade primária de estabelecer e monitorar controles eficazes para deter e detectar fraudes, a atividade de auditoria interna é obrigada a avaliar o risco de fraude, de acordo com as *Normas Internacionais para a Prática Profissional de Auditoria Interna*. Adicionalmente, o *chief audit executive* (CAE) deve reportar questões significantes de risco e controle, incluindo fraudes, à alta administração e ao conselho (Norma 2060 – Reporte para a Alta Administração e o Conselho).

As *Normas* exigem que a atividade de auditoria interna avalie os riscos de fraude nos níveis organizacional e do trabalho. Para garantir a revisão adequada dos riscos relevantes a cada trabalho, os auditores internos devem conduzir uma avaliação de risco de fraude como parte do planejamento do trabalho (Norma 2210.A1). Ao longo do tempo, o conhecimento que a atividade de auditoria interna obtém durante trabalhos individuais pode ser compilado na forma de uma avaliação mais robusta e abrangente do risco de fraude em toda a organização.

Este guia prático descreve as características da fraude e do processo de identificação e avaliação dos riscos de fraude durante o planejamento do trabalho. O processo exato de incorporação da avaliação do risco de fraude no planejamento do trabalho pode variar de acordo com as necessidades específicas da organização, da atividade de auditoria interna e do trabalho. No entanto, o processo geralmente inclui os seguintes passos:

- Coletar informações para entender o propósito e o contexto do trabalho, assim como a governança, gerenciamento de riscos e controles relevantes para a área ou processo sob revisão.
- Fazer um *brainstorming* de cenários de fraude, para identificar possíveis riscos de fraude.
- Avaliar os riscos de fraude identificados, para determinar quais riscos demandam atenção adicional durante o trabalho.

Introdução

A atividade de auditoria interna é responsável por avaliar os processos de gerenciamento de riscos da organização e sua eficácia, incluindo a avaliação dos riscos de fraude e de como eles são geridos pela organização (2120.A2). No entanto, avaliar o potencial de ocorrência de fraude durante o planejamento de cada trabalho é igualmente importante, porque novos riscos de fraude pode surgir a qualquer momento. Portanto, os auditores internos devem considerar a probabilidade de fraude quando desenvolverem os objetivos de cada trabalho (Norma 2210.A2).

Realizar uma avaliação do risco de fraude no início de um trabalho permite aos auditores internos descobrir riscos de fraude que possam não ter estado presentes na última atualização da avaliação de riscos de toda a organização. Adicionalmente, riscos de fraude que possam ser irrelevantes no nível organizacional podem ter significância em uma área ou processo individual.

Embora os auditores internos devam ter conhecimento suficiente para avaliar o risco de fraude e como ele é gerido pela organização, não se espera que tenham a expertise de uma pessoa cuja principal responsabilidade seja detectar e investigar fraudes (Norma 1210.A2). Ao avaliar o risco de fraude, espera-se que os auditores internos se utilizem do zelo profissional devido (Norma 1220.A1) e mantenham uma conduta justa e imparcial (Norma 1120 – Objetividade Individual). Os auditores internos também demonstram o ceticismo profissional – uma atitude inquisitiva, livre de parcialidade ou suposições sobre a honestidade inerente da administração ou dos funcionários –, porque isso permite uma avaliação objetiva e crítica da área ou processo sob revisão.

Este guia prático oferece uma breve visão geral das características da fraude, seguida de uma descrição de como avaliar os riscos de fraude como parte do planejamento do trabalho. O guia descreve como coletar informações, fazer *brainstorming* de cenários de fraude, identificar riscos de fraude e classificar sua importância, para determinar quais riscos de fraude devem ser avaliados adicionalmente durante o trabalho.

Entendendo a Fraude

Embora existam muitas definições, o The IIA define *fraude* como "quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança". A definição representa a característica que a torna única entre os demais riscos: a intenção. Atos fraudulentos envolvem pessoas com intenção de contornar os controles ou explorar as fraquezas da organização. A definição do The IIA também observa que "fraudes são perpetradas a fim de se obter dinheiro, propriedade ou serviços; para evitar pagamento ou perda de serviços; ou para garantir vantagem pessoal ou em negócios".

Como a legislação varia, a legalidade de um ato fraudulento pode ser questionável. Por exemplo, uma organização multinacional com sede em um país em que um ato é ilegal pode conduzir seu negócio em outros países em que o mesmo ato não viola as leis locais. Não importa quais sejam as distinções legais, o propósito de uma avaliação do risco de fraude é identificar o potencial de violações de confiança, explorações de fraquezas e os desvios dos controles.

Três fatores estão consistentemente presentes quando pessoas cometem fraudes: pressão ou incentivo, oportunidade percebida e racionalização.[1]

Pressão ou Incentivo – Uma necessidade real ou percebida que oferece razão ou motivo, como:

- A necessidade de atingir metas de desempenho organizacional ou metas financeiras.
- Dificuldades pessoais ou fatores externos de estresse (ex., problemas financeiros, de saúde ou vícios).
- O desejo de ganhar poder, influência ou estima perante a família, amigos, colegas ou a administração (ex., hackers que cometem fraude, buscando exibir suas capacidades, em vez de causar danos).

Oportunidade – Uma combinação de circunstâncias ou condições que permitem que a fraude ocorra, como:

- Desenvolvimento inapropriado dos controles, falta de controles, segurança ou segregação de deveres insuficiente, ou outras circunstâncias que possam permitir uma falha de controle.
- Um nível de confiança, autoridade, conhecimento e/ou acesso a processos de controle que permita que os funcionários contornem ou sobrescrevam controles existentes.
- Supervisão, treinamento ou comunicação inadequada, quanto às políticas de conduta profissional e às consequências das violações.

[1] Cressey, D.R. "The Criminal Violation of Financial Trust," *American Sociological Review*, 15, nº 6 (1950): 738-743.

Racionalização – Uma justificativa fabricada, convincente e plausível, como:

- Sentimentos de merecimento, devido ao comprometimento organizacional (ex., efetivação, horas excessivas de trabalho não pagas ou desempenho não recompensado).
- Crença de que as ações sejam aceitáveis, porque "os outros provavelmente também fazem."
- Crença de que as ações sejam aceitáveis, porque são culturalmente comuns ou foram consideradas aceitáveis em organizações anteriores.
- Crença de que políticas e procedimentos não fazem sentido ou não têm justificativa.
- Raciocínio de que as ações são temporárias e/ou um evento isolado (ex., "estou pegando dinheiro emprestado e vou devolver" ou "só dessa vez").
- Crença de que a ação não tenha vítimas ou seja tão insignificante que ninguém notaria e/ou se importaria.

Dos três fatores, a oportunidade é a única que as organizações podem controlar diretamente. A administração pode desenvolver controles internos para tentar prevenir oportunidades de fraude e detectar atividades fraudulentas, se ocorrerem.

Os auditores internos devem observar que aqueles que se envolvam em atividades fraudulentas podem racionalizar a fraude não apenas para benefício próprio, mas também para benefício de sua organização ou de um indivíduo ou organização externa. A fraude cometida em benefício à organização é normalmente executada por meio da exploração de uma oportunidade para ganhar vantagem injusta ou desonesta, por meio da enganação de uma parte externa. No entanto, mesmo quando os funcionários usam essa racionalização, eles normalmente recebem um benefício pessoal indireto, como o atingimento de uma meta de desempenho, uma recompensa financeira e/ou uma promoção. O Anexo C lista exemplos de atos fraudulentos e como são racionalizados.

Coletando Informações

Para identificar riscos de fraude na área ou processo sob revisão, os auditores internos devem entender a organização e o contexto amplo em que ela opera (isto é, os ambientes legal, político, social, econômico, de mercado, da indústria e cultural). Adicionalmente, os auditores internos devem entender os objetivos estratégicos e operacionais da organização e como eles estão alinhados com os objetivos da área ou processo sob revisão (Norma 2200 – Planejamento do Trabalho de Auditoria).

Para chegar a esse conhecimento, os auditores internos devem buscar informações a partir de uma variedade de fontes, incluindo:

- Avaliações e investigações anteriores.
- Mecanismos de reporte formais e entrevistas.
- Uma revisão preliminar do ambiente de controle.
- Pesquisa externa e especialistas.

Ao coletar informações para desenvolver uma avaliação do risco de fraude para um trabalho, o papel da atividade de auditoria interna é de avaliar os riscos de fraude relevantes para o trabalho, em vez de investigar uma fraude em potencial. Portanto, os auditores internos devem se comunicar discretamente, manter a confidencialidade e evitar expressar quaisquer suspeitas ou acusações de fraude. A comunicação descuidada poderia atrapalhar uma possível investigação e apresentar, desnecessariamente, riscos reputacionais e legais indesejados.

Avaliações e Investigações Anteriores

A avaliação de riscos da organização, que documenta os riscos significantes identificados no nível organizacional e forma a base para o plano anual de auditoria interna (Norma 2010.A1), é um bom ponto de partida para a identificação de riscos que poderiam ser relevantes para a área ou processo sob revisão. As avaliações centradas nos riscos de fraude apenas, sejam organizacionais ou limitados à área ou processo sob revisão, também podem ser fontes úteis de informação. Os auditores internos devem revisar avaliações relevantes de riscos e investigações de fraude conduzidas pela administração da área sob revisão e por outros prestadores de serviços de avaliação e consultoria, tanto internos quanto externos. Para seres eficientes, os auditores internos tipicamente consideram apenas as avaliações recentes.

Embora as avaliações e investigações anteriores possam oferecer insights valiosos, a importância dos riscos de fraude pode ser afetada por muitos fatores e pode mudar rapidamente. Portanto, conduzir uma avaliação preliminar dos riscos para cada trabalho individual é essencial para o planejamento eficaz do trabalho.

Mecanismos de Reporte Formais e Entrevistas

Os funcionários de uma organização podem oferecer informações úteis sobre os riscos de fraude. Na verdade, a *Association of Certified Fraud Examiners* (ACFE) reporta que, independentemente do porte ou tipo de organização, ou se existe um mecanismo formal de reporte, os funcionários são a fonte de mais de 50 por cento das denúncias de fraude, a forma mais comum de detectar fraudes.[2] Notavelmente, a atividade de auditoria interna foi identificada como o segundo método mais comum de detecção de fraudes.

Muitas organizações estabeleceram mecanismos formais (ex., canais de denúncia, formulários online ou envios de e-mail) para facilitar o reporte de suspeitas de atos fraudulentos e de fraquezas nos controles internos que poderiam expor a organização ao risco de fraude. As preocupações normalmente reportadas incluem alegações de desperdício, abuso de autoridade, apropriação indevida de ativos, conluio e outros comportamentos antiéticos ou suspeitos. Se existir um mecanismo formal de reporte de

[2] Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2016), 20-25, http://www.acfe.com/rttn2016.aspx (acessado em 31 de Outubro de 2017).

fraude, os auditores internos podem pedir ao(s) indivíduo(s) encarregado(s) de sua administração que conceda acesso a quaisquer informações pertinentes à área ou processo sob revisão, como ligações telefônicas gravadas ou declarações documentadas.

Para obter conhecimentos sobre atividades fraudulentas passadas que tenham sido alegadas, descobertas e/ou investigadas, os auditores internos normalmente questionam outros funcionários responsáveis pela gestão dos riscos, alegações e ocorrências de fraude. Tais funcionários podem incluir conselheiros legais, recursos humanos, executivos de ética, executivos de risco e conformidade, segurança e gerenciamento do risco de fraude.

Adicionalmente, entrevistar funcionários de todos os níveis da área ou processo sob revisão pode trazer informações valiosas que não seriam disponibilizadas de outra forma. Os indivíduos que realizam as tarefas e funções diárias da área ou processo sob revisão frequentemente oferecem a descrição mais precisa e atualizada de como o processo e controles relevantes *realmente* funcionam, em comparação com a forma como *deviam* funcionar. Entender as operações reais pode revelar diversas formas de contornar os controles. Para identificar possíveis entrevistados, os auditores internos podem consultar um diagrama organizacional com os cargos e responsabilidades dos funcionários da área sob revisão ou um mapa de processo com uma lista dos principais controles (seja ele oferecido pela administração ou criado pela atividade de auditoria interna).

Possíveis Frases de Alerta

Certas frases usadas pelos entrevistados podem indicar possíveis deficiências de controle e/ou riscos de fraude:

- “Como solução alternativa...”
- “Apenas dessa vez...”
- “Sempre fiz assim.”
- “De vez em quando,...”
- “Extraoficialmente,...”
- “Não há políticas ou procedimentos para esse processo.”
- “Disseram-me para fazer assim; no entanto, não sei por quê.”
- “É assim que é *realmente* feito.”
- “A forma como *devia* funcionar...”

O Anexo D lista possíveis palavras de alerta.

Revisão Preliminar do Ambiente de Controle

Mecanismos formais de reporte e entrevistas frequentemente expõem questões relativas ao ambiente de controle da organização que poderiam levar à fraude. Alertas adicionais podem ser descobertos por meio de uma revisão dos elementos do ambiente de controle, como a estrutura e os valores éticos da organização, assim como a filosofia e estilo operacional da administração. Uma avaliação do ambiente de controle deve incluir a avaliação da maturidade do ambiente de controle e da eficácia dos controles relevantes. A avaliação pode revelar possíveis motivadores comportamentais e/ou pressões que poderiam levar os funcionários a racionalizar a execução de uma fraude. Por exemplo, os funcionários podem

expressar ciência sobre as pressões com o desempenho ou preocupações com metas não realistas que indivíduos poderiam usar para justificar comportamentos fraudulentos. Para obter conhecimento sobre possíveis pressões, os auditores internos devem identificar as metas e métricas de desempenho (isto é, *key performance indicators*) e incentivos relacionados na área sob revisão.

Como os auditores internos têm uma visão holística da organização e de seu ambiente de controle, eles podem ficar cientes de mudanças culturais na organização ao longo do tempo. Mudanças culturais poderiam aumentar a probabilidade de ocorrência de fraude e passar despercebidas. No nível do trabalho, os auditores internos podem estar mais próximos das operações detalhadas, sistemas e pessoal da área ou processo sob revisão do que a alta administração (e de outros que gerenciem os riscos de fraude da organização). Portanto, é vital que os auditores internos estejam alertas às palavras e ações dos funcionários que possam indicar fraquezas no ambiente de controle. Se houver suspeita de fraquezas no ambiente de controle, o supervisor do trabalho deve comunicar a informação ao CAE, porque a questão pode ir além do escopo do trabalho. O Guia Prático do The IIA "*Auditing the Control Environment*" cobre este tópico em maiores detalhes.

Possíveis Alertas

Problemas de Administração:

- Falta de expertise na área
- Falta de supervisão
- Histórico de violações legais

Problemas de Pessoal:

- Falta de verificações de histórico
- Funcionários insatisfeitos
- Falta de disposição para compartilhar deveres

Problemas de Processo:

- Deveres não segregados
- Má segurança física
- Controles de acesso indevidos

Pesquisa Externa e Especialistas

Os auditores internos não são obrigados a ter a expertise de um investigador especializado em fraudes. No entanto, devem ter conhecimento suficiente para avaliar o risco de fraude e a maneira como ele é gerido pela organização (Norma 1210.A2). Os auditores internos podem obter tal conhecimento, pesquisando fraudes que tenham ocorrido em organizações ou indústrias parecidas e estudando tendências de fraude. Além disso, os auditores internos podem usar referências de benchmarking para comparar as práticas de gerenciamento do risco de fraude da organização e da área sob revisão com aquelas de organizações comparáveis e/ou mais amadurecidas. O conhecimento também pode ser adquirido através da leitura de publicações, de manter-se atualizado quanto às mudanças nos regulamentos e do comparecimento a conferências e treinamentos. Organizações profissionais relevantes frequentemente oferecem tais ferramentas e informações, assim como normas profissionais.

O CAE deve garantir que a atividade de auditoria interna possua ou obtenha, coletivamente, as competências necessárias para cumprir com suas responsabilidades (Norma 1210 – Proficiência) e deve obter orientações competentes e assistência, caso os auditores internos não tenham as competências necessárias para conduzir todo ou parte do trabalho (Norma 1210.A1). Além de oferecer oportunidades de treinamento e *mentoring* para a equipe de auditoria interna, o CAE pode solicitar especialistas com conhecimento da indústria ou de áreas ou processos funcionais específicos. Ao realizar sessões de brainstorming de cenários de fraude ou um trabalho que inclua riscos de fraude, os auditores internos podem consultar tais especialistas, conforme necessário.

Brainstorming de Cenários de Fraude

Com base nas informações coletadas, os auditores internos podem começar a contemplar possíveis cenários e riscos de fraude relevantes para a área ou processo sob revisão. O brainstorming de cenários de fraude é uma forma eficaz de determinar as características e circunstâncias únicas da área ou processo específico sob revisão que podem produzir oportunidades e incentivos à fraude.

A necessidade de sessões de brainstorming, a complexidade das sessões e os participantes envolvidos variam de um trabalho para o outro, dependendo das necessidades da atividade de auditoria interna, da organização e do trabalho, assim como do conhecimento dos auditores internos sobre a área ou processo sob revisão. Para elaborar uma lista precisa de cenários de fraude, os auditores internos devem fazer o brainstorming com indivíduos de conhecimentos, perspectivas e relacionamentos diversificados com a área ou processo sob revisão.

Possíveis Participantes para o Brainstorming

- Contabilidade e Finanças
- Auditoria Interna
- Jurídico e Conformidade
- Operacional
- Proprietários dos Processos
- Alta Administração
- Outros Prestadores de Serviços de Avaliação

No brainstorming dos riscos de fraude, os participantes devem considerar as possíveis pressões e oportunidades para cometer fraudes na área ou processo sob revisão. Os participantes também devem considerar cenários de fraude que envolvam ameaças de TI internas e externas, como acesso para sobrescrever configurações do sistema, o que poderia permitir transações fraudulentas e/ou o roubo de informações organizacionais confidenciais.

O brainstorming tem o objetivo de encorajar a participação aberta e o compartilhamento de ideias e pensamentos sem inibição. Portanto, ao revisão os cenários de fraude propostos, os auditores internos devem reconhecer que alguns possíveis riscos de fraude podem ser altamente improváveis, podem não estar bem alinhados com os objetivos do trabalho ou podem estar fora do escopo e alocação de recursos do trabalho atual.

As informações coletadas durante as sessões de brainstorming poderiam ser usadas para desenvolver uma lista de cenários e riscos de fraude em qualquer área ou processo auditável. Para ilustrar, a **Figura 1** apresenta cenários de fraude e riscos correspondentes que poderiam ser identificados durante uma sessão de brainstorming para um trabalho de avaliação de contas a pagar. O Anexo E mostra uma avaliação de riscos de fraude em um trabalho do processo de despesas em dinheiro.

Figura 1: Brainstorming de Cenários de Fraude

Cenário de Fraude	Risco de Fraude
A. Gastos fictícios dos funcionários.	A.1 Cartões corporativos são emitidos indevidamente de propósito, resultando em gastos fraudulentos.
	A.2 Gastos são registrados para bens ou serviços que não foram realmente prestados à organização.
	A.3 Diversos ressarcimentos de gastos são registrados para o mesmo gasto.
B. Despesas fraudulentas.	B.1 Fornecedores fictícios são cadastrados no sistema, resultando em pagamentos fraudulentos.
	B.2 Reembolsos falsos e/ou nulos são processados.
C. Passivos e gastos ocultos.	C.1 Gastos de insolvência são omitidos intencionalmente.
	C.2 Os gastos são capitalizados.
D. Transações entre partes relacionadas.	D.1 Uma parte recebe algum benefício que não seria possível em uma transação entre partes não relacionadas.
E. Peculato	E.1 Funcionários pagam despesas pessoais com os fundos da organização e falsificam os registros financeiros para encobrir o ato.

Avaliando Riscos de Fraude

Como o trabalho não pode cobrir todo risco, os auditores internos avaliam a importância dos riscos de fraude identificados durante o brainstorming, para determinar quais devem ser avaliados adicionalmente durante o trabalho. Uma forma eficaz de conduzir e documentar a avaliação de riscos de fraude é criar uma matriz de riscos de fraude, listando os cenários de fraude e os riscos relevantes e, então, expandindo a matriz para incluir métricas de importância.

Uma matriz de riscos de fraude pode ser criada usando uma planilha ou documento semelhante, com ou sem um software de auditoria. O formato da matriz pode variar, mas, normalmente, inclui uma linha para cada risco e uma coluna para cada métrica de risco, como impacto e probabilidade.

A **Figura 2** ilustra como os cenários de risco documentados na Figura 1 poderiam ser expandidos para incluir as classificações dos riscos por impacto e probabilidade.

Avaliar o impacto pode ser complicado, porque ele envolve fatores quantitativos e qualitativos. Os auditores internos devem considerar não apenas o impacto financeiro, operacional e regulatório dos possíveis riscos de fraude, mas também os impactos não financeiros, como danos à reputação da organização ou aos relacionamentos com clientes ou fornecedores. Por exemplo, um risco de fraude com impacto financeiro direto não material para a organização ainda poderia afetar amplamente sua reputação e, portanto, poderia ser categorizado como de alto impacto.

Figura 2: Matriz de Riscos de Fraude de Contas a Pagar

Cenário de Fraude	Risco de Fraude	Impacto (B, M, A)	Probabilidade (B, M, A)
A. Gastos fictícios dos funcionários.	A.1 Cartões corporativos são emitidos indevidamente de propósito, resultando em gastos fraudulentos.	B	M
	A.2 Gastos são registrados para bens ou serviços que não foram realmente prestados à organização.	A	M
	A.3 Diversos ressarcimentos de gastos são registrados para o mesmo gasto.	M	A
B. Despesas fraudulentas.	B.1 Fornecedores fictícios são cadastrados no sistema, resultando em pagamentos fraudulentos.	A	A
	B.2 Reembolsos falsos e/ou nulos são processados.	B	A
C. Passivos e gastos ocultos.	C.1 Gastos de insolvência são omitidos intencionalmente.	A	B
	C.2 Os gastos são capitalizados.	A	B
D. Transações entre partes relacionadas.	D.1 Uma parte recebe algum benefício que não seria possível em uma transação entre partes não relacionadas.	M	M
E. Peculato	E.1 Funcionários pagam despesas pessoais com os fundos da organização e falsificam os registros financeiros para encobrir o ato.	M	M

Os fatores a considerar na avaliação da probabilidade incluem alegações ou ocorrências anteriores de fraude, a predominância de fraudes semelhantes na indústria e a complexidade e número de pessoas envolvidas no processo.

As classificações de risco da matriz de riscos de fraude podem ser representadas em um gráfico básico, como um mapa de calor. Ao plotar o impacto de cada risco em um eixo e sua probabilidade no outro, os auditores internos ilustram claramente a importância geral, ou prioridade, do risco. Normalmente, a importância combinada de impacto e probabilidade é indicada usando um sistema de cor: vermelho denota as prioridades mais altas, laranja denota os riscos que são significantes o suficiente para serem considerados e amarelo denota os riscos que não são significantes.

A **Figura 3** mostra um mapa de calor criado a partir das informações na matriz de riscos de fraude apresentada na Figura 2. O mapa de calor deve ser incluído nos papéis de trabalho do projeto, porque apoia as decisões dos auditores internos sobre a importância dos riscos.

Uma limitação do mapa de calor é que impacto e probabilidade parecem ser igualmente importantes. Embora tal equivalência possa ser verdadeira às vezes, o impacto normalmente tem prioridade em relação à probabilidade. Por exemplo, na maioria dos casos, um risco que é definido como de alto impacto e de baixa probabilidade (H, L) deve ser priorizado em relação a um risco considerado de baixo impacto, mesmo que a probabilidade seja alta (L, H).

Uma limitação adicional do mapa de calor é que ele mostra apenas duas variáveis por vez (nesse caso, impacto e probabilidade). Pode ser desejável ou necessário considerar também métricas como velocidade, vulnerabilidade, volatilidade, interdependência e/ou correlação ao determinar a importância do risco.

Com base no mapa de calor completo, os auditores internos podem facilmente visualizar os riscos de fraude significantes que devem ser incluídos no trabalho para exames adicionais. A **Figura 4** mostra a matriz de riscos de fraude ajustada, para refletir apenas os riscos de fraude priorizados no exemplo do trabalho de contas a pagar.

Os auditores internos podem oferecer à administração os riscos de fraude identificados a serem considerados para inclusão na avaliação de riscos da organização.

Figura 3: Mapa de Calor

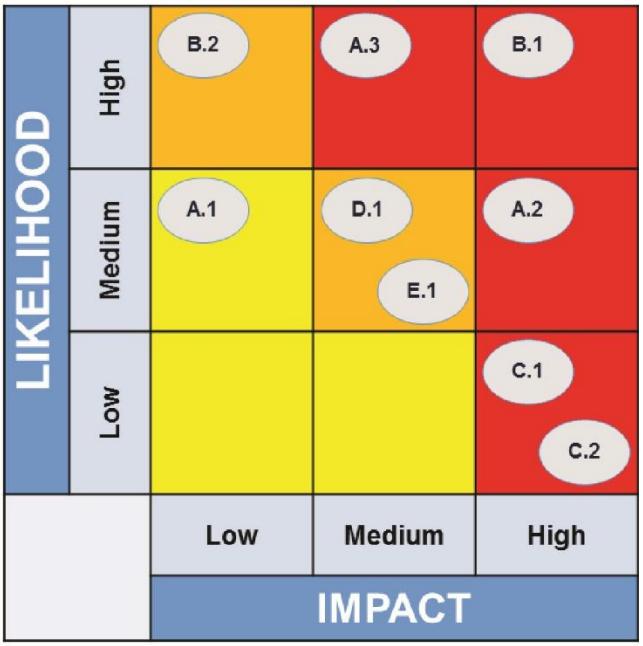

Figura 4: Riscos Significantes de Fraude

Risco de Fraude	Impacto (B, M, A)	Probabilidade (B, M, A)
B.1 Fornecedores fictícios são cadastrados no sistema, resultando em pagamentos fraudulentos.	A	A
A.2 Gastos são registrados para bens ou serviços que não foram realmente prestados à organização.	A	M
A.3 Diversos ressarcimentos de gastos são registrados para o mesmo gasto.	M	A
C.1 Gastos de insolvência são omitidos intencionalmente.	A	B
C.2 Os gastos são capitalizados.	A	B
D.1 Uma parte recebe algum benefício que não seria possível em uma transação entre partes não relacionadas.	M	M
E.1 Funcionários pagam despesas pessoais com os fundos da organização e falsificam os registros financeiros para encobrir o ato.	M	M

Os riscos de fraude que não forem selecionados para exames adicionais durante este trabalho podem ser transferidos para o inventário de riscos de fraude da auditoria interna, ou lista de observação, para que sejam considerados em futuros trabalhos.

Se as informações descobertas durante a avaliação de riscos de fraude indicarem um possível ato fraudulento, os auditores internos devem seguir os protocolos estabelecidos de reporte interno e de investigação de alegações de fraude. Normalmente, os auditores internos reportam a preocupação e evidências preliminares ao CAE, que, então, decide se a questão precisa ser passada para a alta administração e/ou para o conselho.

Identificando Controles

Depois que os auditores internos considerarem os cenários de risco e identificarem e priorizarem os riscos de fraude, eles devem determinar quais controles, se houver, estão em prática para mitigar esses riscos.

Figura 5: Matriz de Riscos e Controles de Fraude para Contas a Pagar

Risco de Fraude	Impacto (B, M, A)	Probab. (B, M, A)	Controle
B.1 Fornecedores fictícios são cadastrados no sistema, resultando em pagamentos fraudulentos.	A	A	Segregação de deveres na gestão de fornecedores.
A.2 Gastos são registrados para bens ou serviços que não foram realmente prestados à organização.	A	M	Confirmação de recebimento de bens e serviços.
A.3 Diversos ressarcimentos de gastos são registrados para o mesmo gasto.	M	A	Controles automatizados para detectar envios duplicados de despesas.
C.1 Gastos de insolvência são omitidos intencionalmente.	A	B	Monitoramento e aprovação regulares de cálculos de gastos de insolvência.
C.2 Os gastos são capitalizados.	A	B	Revisão e aprovação por parte da gerência de todas as entradas de capitalização.
D.1 Uma parte recebe algum benefício que não seria possível em uma transação entre partes não relacionadas.	M	M	*Due diligence* para transações entre partes relacionadas.
E.1 Funcionários pagam despesas pessoais com os fundos da organização e falsificam os registros financeiros para encobrir o ato.	M	M	Segregação de deveres em contas a pagar e aprovação da gerência necessária para despesas do pessoal.

A **Figura 5** ilustra a expansão da matriz da Figura 4 para incluir os controles existentes. Como o mapa de calor, a matriz de riscos e controles de fraude deve ser incluída nos papéis de trabalho do projeto. As informações da matriz são, então, incorporadas à avaliação preliminar de riscos usada para estabelecer os objetivos e escopo do trabalho. O Guia Prático do The IIA "*Engagement Planning: Establishing Objectives and Scope*" oferece informações detalhadas sobre trabalhar em cima da avaliação de riscos para desenvolver os objetivos e escopo do trabalho. Além disso, o mapa de calor de riscos de fraude e a matriz de riscos e controles apoiarão os resultados e conclusões do trabalho, em conformidade com a Norma 2330 – Documentação das Informações.

Anexo A. Normas e Orientações do The IIA

Normas Relevantes do The IIA

As seguintes seleções das *Normas Internacionais para a Prática Profissional de Auditoria Interna* relevantes para o Planejamento do Trabalho: Avaliando Riscos de Fraude. Por favor, consulte as *Normas* para o conteúdo completo. Para auxiliar com a implementação das *Normas*, o The IIA recomenda que os auditores internos consultem o Guia de Implantação respectivo de cada norma.

1210 – Proficiência

1210.A1

1210.A2

1220 – Zero Profissional Devido

1220.A1

2120 – Gerenciamento de Riscos

2120.A2

2200 – Planejamento do Trabalho de Auditoria

2210 – Objetivos do Trabalho de Auditoria

2210.A1

2210.A2

Orientações Relacionadas do The IIA

Guia Prático, *"Auditing the Control Environment."*

Guia Prático, *"Engagement Planning: Establishing Objectives and Scope."*

Guia Prático, *"Internal Auditing and Fraud."*

Anexo B. Glossário

Termos identificados com um asterisco (*) foram retirados da edição de 2017 do Glossário do *International Professional Practices Framework* do The IIA.

Ambiente de Controle* – Atitudes e ações do conselho e da administração, em relação à importância dos controles dentro da organização. O ambiente de controle proporciona a disciplina e a estrutura para se atingirem os principais objetivos do sistema de controle interno. O ambiente de controle inclui os seguintes elementos:

- Integridade e valores éticos.
- Filosofia e estilo operacional da administração.
- Estrutura organizacional.
- Atribuição de autoridade e responsabilidade.
- Políticas e práticas de recursos humanos.
- Competência do pessoal.

Controle* – Qualquer ação tomada pela administração, conselho ou outras partes para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos serão alcançados. A administração planeja, organiza e dirige a execução de ações suficientes para prover razoável certeza de que os objetivos e metas serão alcançados.

Fraude* – Quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o 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 para garantir vantagem pessoal ou em negócios.

Risco* – A possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade.

Anexo C. Exemplos de Atos Fraudulentos

Os exemplos de atos fraudulentos a seguir não compõem uma lista completa ou priorizada. Em vez disso, são oferecidos para estimular a conscientização de riscos de fraude em potencial, categorizados por tipo de racionalização.

Exemplos de fraude cometida para benefício direto de um indivíduo incluem:

- Desvio intencional de receita para um funcionário, parte interessada ou parte externa que normalmente geraria lucros para a organização.
- Peculato (ex., apropriação indevida de dinheiro ou propriedade e falsificação de registros financeiros para encobrir o ato).
- Espionagem, incluindo pesquisa e desenvolvimento.
- Ocultação intencional ou representação indevida de eventos, transações ou dados.
- Pagamentos realizados por serviços ou bens não realmente prestados à organização.
- Não agir, em situação em que uma ação seja exigida pela organização ou pela lei.
- Uso ilegal ou não autorizado de informações confidenciais ou proprietárias.
- Manipulação ilegal ou não autorizada de redes de TI ou sistemas operacionais.
- Roubo.
- Aceitação de subornos ou propinas.

Exemplos de fraude que beneficiariam a organização diretamente incluem:

- Representação indevida de dados financeiros ou não financeiros, incluindo a valorização de transações, ativos, passivos, rendas ou dados estatísticos (especialmente em fusões e aquisições).
- Preços de transferência (isto é, a valorização de bens trocados entre organizações relacionadas) que permitam que a administração melhore seus resultados em detrimento de organizações concorrentes.
- Atividades de partes relacionadas, em que uma parte receba algum benefício que não seria obtido em uma transação entre partes sem qualquer relacionamento.
- Não registrar ou divulgar informações significantes precisa ou completamente, o que pode proporcionar uma representação melhorada, mas falsa, da organização a partes externas.
- Venda ou atribuição de ativos fictícios ou representados indevidamente.
- Não agir, em situação em que uma ação seja exigida pela organização ou pela lei.
- Distorções significativas nas finanças ou outras atividades de conformidade, para melhorar preços de estoque, ganhar vantagem competitiva ou reduzir impostos ou multas a pagar.
- Atividades comerciais que violem estatutos governamentais, regulamentos ou contratos.
- Contribuições políticas ilegais, subornos e propinas oferecidas a clientes ou fornecedores, ou pagamentos a oficiais do governo ou seus intermediários.

Anexo D. Possíveis Palavras de Alerta a Considerar

A tabela a seguir oferece exemplos de escolhas de vocabulário por parte de entrevistados que podem alertar o ceticismo de um auditor interno em certas circunstâncias ou contextos, justificando, portanto, investigação adicional.

Possíveis Palavras de Alerta a Considerar		
Abordagem Diferente	Difícil	Nova Forma
Agressivo	Em evolução	Possivelmente
Amortecer	Extraoficial	Preocupação
Antecipar	Força	Presumir
Arriscado	Fragmentado	Questão
Às vezes	Freelance	Realocar
Complexo	Incerto	Reservas
Conjuntural	Interpretação	Revisar
Contornar	Máscara/Mascarar	Sob medida
Criativo	Maverick	Suavizar
Depende	Modificar	Subjetivo
Desafiador	Não convencional	Temporário
Desconectar	Não sei	Transição

Anexo E. Estudo de Caso: Trabalho de Avaliação de Despesas em Dinheiro

O estudo de caso a seguir ilustra como riscos de fraude poderiam ser identificados e documentados durante o planejamento de um trabalho de avaliação do processo de despesas em dinheiro. O estudo de caso não cobre todos os riscos de fraude em um processo real de despesas em dinheiro e não tem o objetivo de ser usado como modelo ou programa de avaliação de riscos. Conforme as características de cada organização mudam, também mudam seus riscos de fraude.

Coletando Informações

Durante o planejamento do trabalho de avaliação das despesas em dinheiro, os auditores internos coletaram as seguintes informações:

- Não há registro de avaliações internas ou externas ou de investigações anteriores.
- Os funcionários com a habilidade de atualizar informações dos fornecedores no arquivo mestre de fornecedores também têm a habilidade de processar pagamentos no sistema.
- Diversos funcionários têm acesso de superusuário a funções de contas a pagar: gerenciar o arquivo mestre de fornecedores, gerar faturas, contornar a aprovação de faturas e atualizar informações de pagamento.
- O fluxograma de aprovação é aplicado inconsistentemente e frequentemente contornado no sistema.
- As revisões e aprovações das despesas são feitas inconsistentemente.
- A receita diminuiu significativamente em relação ao ano anterior, embora as despesas operacionais tenham aumentado inesperadamente no mesmo período.
- Bonificações são concedidas apenas se as metas financeiras forem atingidas.
- Entrevistas com a equipe de recursos humanos revelaram que o supervisor de contas a pagar foi acusado de fraternização indevida com funcionários que reportam a ele.
- O supervisor é bem amigável e confiante com o pessoal de contas a pagar.

Brainstorming de Cenários de Fraude

Os auditores internos documentaram as seguintes informações durante as sessões de brainstorming de cenários de fraude.

Fatores de Fraude	Cenários de Fraude
Pressão	Bonificações substanciais são concedidas, se as metas financeiras forem atingidas.
	Alguns funcionários estão preocupados com as possibilidades limitadas de ascensão profissional e/ou temem perder seus cargos.
	As bonificações podem não ser pagas esse ano.
	Uma funcionária gabou-se, recentemente, para colegas sobre seu estilo de vida extravagante.
Oportunidade	Os deveres não são devidamente segregados.
	As relações entre os funcionários e a administração podem ser inapropriadas. Uma funcionária tem um relacionamento especialmente próximo com seu gerente.
	Diversos funcionários compartilham o login de acesso de administrador e os dados de processamento de pagamentos e informações bancárias podem ser alterados por funcionários com acesso de administrador.
	O arquivo mestre de fornecedores pode ser atualizado por todos os funcionários e o sistema não monitora o histórico de alterações.
Racionalização	Os funcionários podem perceber favoritismo e podem se sentir desvalorizados e ressentidos.
	Os funcionários podem perceber na administração o reforço de um “tom no topo” negativo.
	Comportamentos indevidos parecem ser comuns.

Avaliando os Riscos de Fraude e Identificando os Controles

Os auditores internos criaram a seguinte matriz de riscos e controles de fraude, para incluir no plano do trabalho.

Cenário de Fraude	Risco de Fraude	Impacto (B, M, A)	Probabilidade (B, M, A)	Controle
A. Fornecedores não aprovados	A.1 Fornecedores fictícios são configurados no sistema, o que pode resultar em pagamentos fraudulentos.	A	A	• Segregação de deveres. • Revisão periódica do arquivo mestre de fornecedores.
	A.2 Os endereços dos fornecedores são substituídos por endereços dos funcionários; ou as informações de pagamento são trocadas pelas contas bancárias dos funcionários.	M	M	• A aprovação da gerência é necessária para alterações nos endereços dos fornecedores e dados de transferências eletrônicas de fundos.
B. Pagamentos Indevidos	B.1 Reembolsos fictícios são processados para pagamento.	M	M	• A aprovação da gerência é necessária para despesas.
	B.2 Aprovações de faturas fictícias ou duplicadas são passadas no sistema.	A	A	• A aprovação da gerência é necessária antes que o pagamento possa ser processado.
C. Conluio	C.1 O supervisor está em conluio com um funcionários para contornar os controles existentes.	A	M	• Nenhum

Incorporando os Resultados no Plano de Trabalho

Depois de criar a matriz de riscos e controles de fraude, os auditores internos incorporaram a avaliação de riscos de fraude e as descobertas preliminares ao plano de trabalho da avaliação das despesas em dinheiro, juntamente com as seguintes observações:

- Revisar o arquivo mestre de fornecedores com nomes e endereços, para verificar a existência de fornecedores que aparentem estar duplicados.
- Examinar nomes parecidos de fornecedores com endereços e/ou informações de pagamento diferentes.
- Verificar endereços e informações bancárias dos fornecedores, em busca de correspondências com dados de funcionários.
- Buscar endereços de fornecedores que pareçam ser residenciais ou caixas postais.
- Revisar o histórico de faturas e quantias pagas correspondentes, em busca de números duplicados de faturas ou quantias pagas em repetição.
- Acompanhar o processo de pagamento e buscar questões de segregação de deveres quanto às aprovações.

Agradecimentos

Equipe de Desenvolvimento de Orientações

Glenn Ho, CIA, CRMA, África do Sul (Presidente)

Doug Hileman, CRMA, CPEA, Estados Unidos (Líder de Projeto)

Caroline Glynn, CIA, Estados Unidos

John Mickevice, CIA, CRMA, Estados Unidos

Daniel Samson, CIA, Estados Unidos

Contribuintes às Orientações Globais

Awad Elkarim Mohamed Ahmed, CIA, CCSA, CFSA, CGAP, CRMA, Emirados Árabes Unidos

Elastos Chimwanda, CIA, Zimbabwe

Dana Lawrence, CIA, CFSA, CRMA, Estados Unidos

Barry Smit, CIA, África do Sul

Dr. Gokhan Sungun, CIA, CCSA, CRMA, Estados Unidos

Oliver Sznitkies, França

Normas e Orientações Globais do The IIA

Christine Hovious, CIA, CRMA, Diretora (Líder de Projeto)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice-Presidente

Debi Roth, CIA, Diretora Geral

Lauressa Nelson, Redatora Técnica

Christina Brune, Redatora Técnica

O The IIA gostaria de agradecer aos seguintes órgãos de supervisão por seu apoio: Guidance Development Committee, *Professional Guidance Advisory Council*, *International Internal Audit Standards Board*, *Professional Responsibility and Ethics Committee* e *International Professional Practices Framework Oversight Council*.

Sobre o Instituto

The Institute of Internal Auditors (The IIA) é o mais reconhecido advogado, educador e fornecedor de normas, orientações e certificações da profissão de auditoria interna. Fundado em 1941, o The IIA atende, atualmente, mais de 195.000 membros de mais de 170 países e territórios. A sede global da associação fica em Lake Mary, na Flórida. Para mais informações, visite www.globaliia.org ou www.theiia.org.

Sobre as Orientações Suplementares

Orientações Suplementares fazem parte do *International Professional Practices Framework* (IPPF) do The IIA e oferecem orientações adicionais recomendadas (não obrigatórias) para a condução de atividades de auditoria interna. Embora apoiem as *Normas*, as Orientações Suplementares não têm o objetivo de relação direta com o atingimento da conformidade com as *Normas*. Elas têm o objetivo de abordar tópicos específicos, assim como questões específicas de determinados setores, e incluem processos e procedimentos detalhados. Esta orientação é apoiada pelo The IIA, por meio de processos formais de revisão e aprovação.

Guias Práticos

Os Guias Práticos são um tipo de Orientação Suplementar, que fornecem 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 entregáveis. Como parte das orientações do IPPF, a conformidade com os Guias Práticos é recomendada (não obrigatória). Os Guias Práticos são apoiados pelo The IIA, por meio de processos formais de revisão e aprovação.

Um *Global Technologies Audit Guide* (GTAG) é um tipo de Guia Prático, redigido em linguagem clara de negócios, para abordar uma questão tempestiva relativa ao gerenciamento, controle ou segurança da tecnologia da informação.

Para mais materiais de orientação fidedignos fornecidos pelo The IIA, por favor, visite nosso site em www.globaliia.org/standards-guidance ou www.theiia.org/guidance.

Isenção de Responsabilidade

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

Copyright

Outubro de 2017