

Prevenção e Detecção de Fraudes em um Mundo Automatizado

Tradução ao Português Patrocinada pela:

Global Technology Audit Guide (GTAG)

Redigida em linguagem clara de negócios para abordar uma questão tempestiva relativa ao gerenciamento, controle ou segurança da TI, a série GTAG serve como pronto recurso para *chief audit executives* sobre diferentes riscos associados à tecnologia e práticas recomendadas.



Controles de Tecnologia da Informação: Os tópicos discutidos incluem conceitos de controle de TI, a importância dos controles de TI, os papéis e responsabilidades organizacionais para garantir controles eficazes de TI e técnicas de análise e monitoramento de riscos.



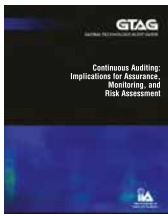
Terceirização da Tecnologia da Informação: Discute como escolher o fornecedor terceirizado de TI correto e as principais considerações de controle de terceirização sobre a operação do cliente e sobre a operação do prestador de serviços.



Controles de Gestão de Mudanças e Patches: descreve as fontes de mudança e seu possível impacto sobre os objetivos do negócio, além de como os controles de gestão de mudanças e *patches* ajudam a gerenciar os riscos e custos de TI e o que funciona e não funciona na prática.



Auditando Controles de Aplicativos: Aborda o conceito de controle de aplicativos e sua relação com os controles gerais, além de como definir o escopo de uma revisão de controle de aplicativos baseada em riscos.



Auditoria Contínua: Aborda o papel da auditoria contínua no ambiente de auditoria interna atual; a relação de auditoria contínua, monitoramento contínuo e avaliação contínua; e a aplicação e implementação da auditoria contínua.



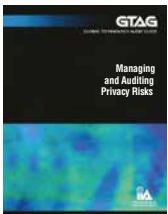
Gestão de Identidades e Acessos: Abrange os principais conceitos relacionados à gestão de identidades e acessos (*identity and access management – IAM*), riscos associados ao processo de IAM, orientações detalhadas sobre como auditar processos de IAM e uma amostra de checklist para auditores.



Gerenciamento da Auditoria de TI: Discute os riscos relacionados à TI e define o universo de auditoria de TI, bem como a forma de executar e gerenciar o processo de auditoria de TI.



Gestão de Continuidade de Negócios: Define a gestão de continuidade de negócios (*business continuity management – BCM*), discute os riscos de negócios e inclui uma discussão detalhada dos requisitos do programa de BCM.



Gerenciando e Auditando os Riscos de Privacidade: Discute princípios e estruturas globais de privacidade, modelos e controles dos riscos de privacidade, o papel dos auditores internos, as dez principais perguntas de privacidade a serem feitas durante o curso de uma auditoria e mais.



Desenvolvendo o Plano de Auditoria de TI: Fornece orientações passo a passo sobre como desenvolver um plano de auditoria de TI, desde a compreensão do negócio, a definição do universo de auditoria de TI e a realização de uma avaliação de riscos, até a formalização do plano de auditoria de TI.



Gerenciando e Auditando Vulnerabilidades de TI: Entre outros tópicos, discute o ciclo de vida do gerenciamento de vulnerabilidades, o escopo de uma auditoria de gerenciamento de vulnerabilidades e as métricas para mensurar as práticas de gerenciamento de vulnerabilidades.



Auditando Projetos de TI: Oferece uma visão geral das técnicas para lidar com eficácia com a equipe de projetos e com a administração, para avaliar os riscos relacionados aos projetos de TI.

Visite o site do The IIA em www.theiia.org/technology para baixar toda a série.

Global Technology Audit Guide (GTAG®) 13

Prevenção e Detecção de Fraudes em um Mundo Automatizado

Dezembro de 2009

Copyright © 2009 The Institute of Internal Auditors, 247 Maitland Ave., Altamonte Springs, FL 327014201, EUA. Todos os direitos reservados. Impresso nos Estados Unidos da América. Nenhuma parte desta publicação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma por qualquer meio — eletrônico, mecânico, fotocópia, gravação ou outro — sem a permissão prévia por escrito do editor.

O The IIA publica este documento para fins informativos e educacionais. Este documento destina-se a fornecer informações, mas não substitui a consultoria jurídica ou contábil. O The IIA não fornece tais conselhos e não oferece qualquer garantia quanto a quaisquer resultados jurídicos ou contábeis por meio da publicação deste documento. Quando surgirem problemas jurídicos ou contábeis, deve-se procurar e manter assistência profissional.

Índice

PREFÁCIO	i
SUMÁRIO EXECUTIVO	ii
INTRODUÇÃO.....	1
1.1 Definição de Fraude.....	1
1.2 Normas do The IIA relacionadas à fraude	1
1.3 Usando a Tecnologia para Prevenir e Detectar Fraude.....	1
RISCOS DE FRAUDE DE TI.....	2
2.1 Avaliações de Risco de Fraude de TI	2
2.2 Avaliação de Esquemas de Fraude.....	5
2.3 Esquemas de fraude de TI	5
DETECÇÃO DE FRAUDE USANDO A ANÁLISE DE DADOS	9
3.1 Por Que Usar a Análise de Dados para Detecção de Fraudes?.....	9
3.2 Técnicas Analíticas para Detecção de Fraude	9
3.3 Tipos Típicos de Testes de Fraude.....	9
3.4 Analisando Populações de Dados Completos	11
3.5 Prevenção de Fraudes e Estratégias do Programa de Detecção	11
3.6 Analisando Dados Usando Fontes de Dados Internas e Externas.....	11
O PAPEL DO CAE EM LIDAR COM A FRAUDE DE TI.....	16
4.1 O Comitê de Auditoria.....	16
4.2 Vinte Perguntas que o CAE Deveria Perguntar Sobre Fraude.....	16
REFERÊNCIAS E RECURSOS.....	18
SOBRE OS AUTORES	19

Prefácio

Graças aos implacáveis avanços tecnológicos, praticamente tudo o que encontramos está embutido na tecnologia. Independentemente do setor ou da empresa, a TI é essencial para manter uma vantagem competitiva, gerenciar riscos e alcançar os objetivos de negócios; e organizações do mundo todo estão alocando vastos recursos para projetos tecnológicos vitais.

Conforme a tecnologia avança, também avançam os esquemas para cometer fraudes. A dependência de ferramentas automatizadas para ajudar a perpetuar esses esquemas traz novos desafios para a detecção e prevenção de fraudes.

A fraude, de acordo com o *Black Law Directory*, consiste em “todos os diversos meios que a engenhosidade humana pode conceber e que são usados por um indivíduo para obter uma vantagem sobre outro, por falsas sugestões ou pela supressão da verdade”. A fraude é cara para as organizações e é ruim para a economia. A tecnologia permite que os fraudadores executem e ocultem esquemas de fraude tradicionais com mais facilidade. Por exemplo: os fraudadores podem facilmente produzir um documento falso, como um extrato de conta, para enganar os outros.

A tecnologia também é uma ferramenta que pode ajudar a prevenir e detectar fraudes. Ao usar a tecnologia para implementar programas de prevenção contra fraudes em tempo real e ferramentas avançadas de detecção de fraudes, as organizações podem reduzir o tempo necessário para detectá-las, reduzindo assim seu custo.

É imperativo que os auditores permaneçam à frente dos fraudadores em seus conhecimentos de tecnologia e das ferramentas disponíveis. Com software prontamente disponível, o uso de computadores para isolar as pistas da fraude contábil não só faz sentido, como também é uma necessidade absoluta para que os auditores ajudem a cumprir com seu dever de supervisão independente.

Por todas estas razões, estou especialmente satisfeito com o lançamento do novo GTAG 13 do The IIA: Prevenção e Detecção de Fraudes em um Mundo Automatizado. Essa orientação tempestiva oferece uma visão geral das técnicas para envolver-se, com eficácia, com as equipes e com a administração para avaliar os riscos relacionados à fraude, considerando os avanços tecnológicos. Este Guia Prático inclui:

- Uma explicação dos diversos tipos de análise de dados para uso na detecção de fraudes.
- Uma variedade de riscos de fraude de TI.
- Um modelo de avaliação dos riscos de fraude de TI.

Encorajo você a usar esta orientação fidedigna para fortalecer seu conhecimento sobre a integração entre a tecnologia e a fraude, porque certamente contribuirá para o sucesso dos esforços de detecção de fraude de sua organização!

Scott Grossfeld, CFE, CPA
Chief Executive Officer
Association of Certified Fraud Examiners



Sumário Executivo

A fraude é um risco de negócios que os executivos, especialmente os *chief audit executives* (CAEs), tiveram que enfrentar por muito tempo. Inúmeras manchetes destacaram escândalos e irregularidades corporativas que demonstram a necessidade de que organizações e governos melhorem a governança e a supervisão. Como abordar os riscos de fraude dentro de uma organização de maneira eficaz e eficiente é um importante tópico de preocupação para os conselhos de administração, administração, proprietários de negócios, auditores internos, líderes governamentais, legisladores, reguladores e muitos outros stakeholders. Em muitos casos, novas leis e regulamentos do mundo todo forçaram as organizações a darem uma nova olhada neste problema de longa data.

Apesar de muitas organizações de auditoria interna enfrentarem orçamentos apertados, equipes limitadas e grandes cargas de trabalho, os profissionais de auditoria da atualidade devem ter um papel proativo em ajudar as organizações a gerenciar os riscos de fraude, garantindo que controles apropriados sejam implementados para ajudar a prevenir e detectar fraudes. Para atender às expectativas da administração, dos proprietários de negócios e dos conselhos de administração, os CAEs são desafiados a usar seus recursos disponíveis de maneira eficaz e eficiente. Para esse fim, os auditores internos precisam ter as habilidades apropriadas e devem usar as ferramentas tecnológicas disponíveis para ajudá-los a manter um programa de gestão de fraudes bem-sucedido, que cubra a prevenção, a detecção e a investigação. Como tal, espera-se que todos os profissionais de auditoria – não apenas os especialistas em auditoria de TI – sejam cada vez mais proficientes em áreas como análise de dados e uso da tecnologia, para ajudá-los a atender às demandas do trabalho.

Além de avaliar a adequação dos controles internos, um desafio para os auditores internos é olhar além dos controles e encontrar brechas nos sistemas, nas quais a fraude possa ocorrer. Com um entendimento das relações entre diferentes sistemas e aplicativos de TI, os auditores internos podem aplicar seu raciocínio crítico para identificar áreas de alto risco e detalhar operações específicas.

O objetivo deste GTAG é complementar o Guia Prático do The IIA, *Internal Auditing and Fraud*, e informar e orientar os CAEs e auditores internos sobre como usar a tecnologia para ajudar a prevenir, detectar e responder a fraudes. O guia concentra-se nos riscos de fraude de TI, nas avaliações dos riscos de fraude de TI e em como o uso da tecnologia pode ajudar os auditores internos e outros principais stakeholders da organização a lidar com fraudes e com os riscos de fraude.

1. Introdução

O objetivo deste capítulo é apresentar normas relacionadas à fraude publicadas no *International Professional Practices Framework* (IPPF) do The IIA. O capítulo também define o conceito de fraude e fornece uma visão geral das maneiras pelas quais a tecnologia pode ser implementada para melhorar a prevenção e a detecção de fraudes.

1.1 Definição de Fraude

A fraude engloba uma ampla gama de irregularidades e atos ilegais caracterizados pelo engano intencional ou deturpação. O IPPF do The IIA define fraude como:

“... qualquer ato ilegal caracterizado por engano, ocultação ou violação de confiança. Esses atos não dependem da ameaça de violência ou força física. Fraudes são perpetradas por pessoas e organizações para obter dinheiro, propriedade ou serviços; evitar pagamento ou perda de serviços; ou para garantir vantagem pessoal ou comercial.”

Essa ampla definição de fraude acomoda os riscos de fraude, as exposições e as ameaças encontradas nos departamentos de TI, bem como as fraudes ativadas pelo uso da tecnologia.

1.2 Normas do The IIA relacionadas à fraude

Conforme observado no Guia Prático do The IIA, *Internal Auditing and Fraud*, o The IIA incluiu as normas do IPPF diretamente relacionadas à fraude. As normas a seguir abrangem as funções e responsabilidades dos auditores internos em relação à fraude dentro de uma organização.

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

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

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

2060 – Relatório à Alta Administração e ao Conselho – O *chief audit executive* (CAE) deve reportar periodicamente à alta administração e ao conselho sobre o propósito, a autoridade e a responsabilidade da atividade de auditoria

interna e o desempenho em relação ao seu planejamento. Os reportes devem também incluir questões de riscos e de controles significativos, incluindo os riscos de fraude, os assuntos de governança e outros assuntos que exijam a atenção da alta administração e/ou do conselho.

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

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

1.3 Usando a Tecnologia para Prevenir e Detectar Fraude

Os avanços tecnológicos mais permitem cada vez que as organizações implementem controles automatizados para ajudar a prevenir e detectar fraudes. A tecnologia também permite que as organizações passem de técnicas estáticas ou periódicas de monitoramento de fraudes, como controles detectivos, para técnicas contínuas de monitoramento de fraudes em tempo real, que oferecem o benefício de realmente impedir a ocorrência das fraudes. Este GTAG descreve tanto técnicas de monitoramento periódicas quanto contínuas. Vários pacotes avançados de software analítico estão agora disponíveis para auxiliar na análise de dados. Este GTAG aborda técnicas em geral e não endossa qualquer plataforma específica.

A tecnologia forense de computador e pacotes de software estão disponíveis para ajudar na investigação de fraudes – onde os computadores são usados para facilitar a fraude – ou para identificar sinais de fraude em potencial. A computação forense é uma disciplina investigativa que inclui a preservação, identificação, extração e documentação de hardware e dados de computador para fins de evidência e análise de causa raiz. Exemplos de atividades de computação forense incluem:

- Recuperação de e-mails excluídos.
- Monitoramento de e-mails em busca de indicadores de possíveis fraudes.
- Realização de investigações após demissão.
- Recuperação de evidências após a formatação de um disco rígido.

As atividades forenses de computação ajudam a estabelecer e manter uma cadeia contínua de custódia, o que é crítico para determinar a admissibilidade de provas nos tribunais. Embora o CAE e os auditores internos não devam ser especialistas nesta área, o CAE deve ter um entendimento geral dos benefícios que essa tecnologia proporciona, para que possa contratar especialistas apropriados, conforme necessário, para assistência em uma investigação de fraude.

2. Riscos de Fraude de TI

O objetivo deste capítulo é fornecer informações sobre vários cenários de fraude de TI que podem ocorrer em uma organização. Embora muitos executivos de auditoria, diretores e gerentes provavelmente já tenham um conhecimento prático de riscos e exposições específicos de fraude de TI dentro de sua própria organização, este capítulo discute os tipos de fraude em termos gerais. Portanto, ele não pode abordar situações exclusivas de indústrias ou organizações específicas.

2.1 Avaliações de Risco de Fraude de TI

Conforme estabelecido no Guia Prático do The IIA, *Internal Auditing and Fraud*, todas as organizações estão expostas ao risco de fraude em qualquer processo em que seja necessário o envolvimento humano. A exposição de uma organização a fraudes é uma função dos riscos de fraude inerentes ao negócio; até que ponto existem controles internos eficazes para prevenir ou detectar fraudes; e a honestidade e integridade das pessoas envolvidas no processo. Esses riscos e exposições de fraude se aplicam à TI com a mesma frequência que a qualquer outra área da organização.

A norma de gerenciamento de riscos do IPPF (2120.A2) indica que a atividade de auditoria interna deve avaliar o potencial para a ocorrência de fraude e a maneira pela qual a organização gerencia o risco de fraude. Embora haja várias maneiras de atender a essa norma, é importante que os auditores internos validem que:

- A administração concluiu uma avaliação de riscos de fraude corporativa.
- Todas as áreas significantes da organização foram incluídas na avaliação.
- Elementos-essenciais, como riscos de fraude, controles e lacunas, foram documentados.
- Existe um processo para os esforços de remediação.

Uma avaliação de riscos de fraude de TI é geralmente um componente de um programa mais amplo de gerenciamento de riscos corporativos da organização. Como a administração é responsável pelos programas (de ERM), a gerência de TI deve concentrar esforços para concluir com sucesso a avaliação de riscos de fraude de TI. Em muitas organizações, os auditores internos podem ser solicitados a participar dessas avaliações, devido aos conjuntos de habilidades exclusivas que oferecem à identificação e avaliação de riscos. A avaliação de riscos de fraude de TI é uma ferramenta que ajuda a gerência de TI e os auditores internos a identificar sistematicamente onde e como a fraude pode ocorrer e quem está na posição de cometer fraude. Uma revisão das possíveis exposições a fraudes representa uma etapa essencial no tratamento das preocupações da gerência de TI sobre os riscos de fraude de TI. Semelhante a uma avaliação de riscos corporativos, uma avaliação de riscos de fraude de TI concentra-se em esquemas e cenários de fraude, para determinar a presença de controles internos e se os controles podem ser contornados.

Uma avaliação de riscos de fraude de TI geralmente inclui as seguintes etapas principais:

- Identificar fatores relevantes de riscos de fraude de TI.
- Identificar possíveis esquemas de fraude de TI e priorizá-los com base na probabilidade e impacto.
- Mapear os controles existentes em busca de possíveis esquemas de fraude e identificação de lacunas.
- Testar a eficácia operacional dos controles de prevenção e detecção de fraudes.
- Avaliar a probabilidade de uma falha de controle e/ou um incidente de fraude e seu impacto sobre os negócios.

As páginas a seguir incluem um modelo ilustrativo de uma avaliação de riscos de fraude de TI:

Proprietário de Negócios	Riscos de Fraude	Controles	Preventivos ou Detectivos	Monitoramento	Probabilidade	Impacto
TI – CIO	Controles físicos insuficientes sobre o hardware de TI resultam em alterações, destruição ou apropriação indebita para ganho pessoal. (Segurança física)	• Hardware de computador crítico localizado em data centers seguros. • Acesso a data centers restritos, com base nas responsabilidades de trabalho. • Diversos esquemas de segurança utilizados (ex., acesso via cartão-chave, vigilância por câmeras de circuito fechado, guardas de segurança). • Políticas e procedimentos documentados. • Manutenção de registros de visitantes. • Cabos de segurança usados para computadores portáteis. • Inventário de estações de trabalho realizado trimestralmente. • Procedimentos de provisionamento formal.	Ambos	• Gestão de data center. • Prevenção de perdas. • Gerenciamento de riscos de TI. • Operações de TI. • Monitoramento diário dos logs de visitantes pela administração. • Inventários periódicos concluídos pela gerência de ativos. • Conciliações financeiras de provisionamento. • Auditoria interna.	Baixo	Alto
TI – CIO	Acesso a sistemas ou dados para ganho pessoal. (Acesso lógico) a) Acesso a informações pessoais de clientes ou funcionários (ex., informações de cartão de crédito, informações de folha de pagamento). (Roubo de identidade) b) Acesso a informações confidenciais da empresa (ex., relatórios financeiros, dados de fornecedores, planos estratégicos). (continua)	• Gestão da identidade: ◦ IDs de usuário individuais atribuídos. ◦ Regras automatizadas de complexidade de senha. ◦ Rotação de senha. • Controles de acesso. • Controles de autenticação. • Controles de autorização: ◦ Os proprietários de negócios aprovam o acesso aos dados. ◦ Listas de controle de acesso. • Políticas e procedimentos documentados • Segregação de deveres. • Equipe de resposta a incidentes em computador. • Controles de rede (ex., firewalls, roteadores). • Acesso remoto seguro. • Gerenciamento de antivírus e <i>patches</i>, para controlar as vulnerabilidades do computador. • IDs restritos de administrador do sistema. • Teste concluído de penetração de rede. (continua)	Ambos	• Segurança da informação. • Administradores do sistema. • Proprietários de negócios. • Auditoria interna.	Médio	Alto

Tabela 1. Modelo Ilustrativo de Avaliação de Riscos de Fraude de TI

GTAG — Riscos de Fraude de TI

Proprietário de Negócios	Riscos de Fraude	Controles	Preventivos ou Detectivos	Monitoramento	Probabilidade	Impacto
	c) Cópia e uso de software ou dados para distribuição. d) Acesso a logs de auditoria ou outros dispositivos de monitoramento usados para detectar problemas para resolução. e) Abuso da rede de telecomunicações.	• Avaliações periódicas de vulnerabilidade de software. • Procedimentos para excluir funcionários demitidos do acesso aos recursos da rede. • Conciliações e revisão de contas. • Violações de segurança registradas e disponíveis para revisão. • Acesso restrito ao código do software. • Dados fictícios usados para testes do sistema. • Linhas dedicadas e criptografadas para transmissão de informações pessoais. • Criptografia <i>Secure Sockets Layer</i> (SSL) para transações on-line.				
TI – CIO	Alterações nos programas ou dados do sistema para ganho pessoal. (Ger. de Alterações)	• Desenvolvimento de sistemas e procedimentos de gestão de projetos. • Procedimentos de gerenciamento de alterações ao sistema. • Segregação de deveres. • Acesso restrito ao ambiente de produção. • Aprovação da administração necessária para alterações ao sistema. • Acesso restrito ao código do software. • Conciliações e revisão de contas.	Ambos	• Gerência de TI. • Administradores do sistema. • Proprietários de negócios. • Gestão financeira. • Auditoria interna.	Baixo	Médio
TI – CIO	Atividade fraudulenta por um contratado independente ou um programador <i>off-shore</i> (ex., cobranças fictícias; apropriação indébita de dados confidenciais de funcionários, clientes ou empresas para ganho pessoal).	• Termos do contrato (ex., informações confidenciais, nenhuma divulgação, devolução de informações confidenciais, direito de auditar). • Acesso restrito, com base nas responsabilidades do trabalho. • Controles de acesso (ex., autenticação e autorização). • As violações de segurança são registradas e estão disponíveis para revisão. • Conciliações e revisão de contas. • Revisão mensal das cobranças do prestador. • Segregação de deveres. • Aprovação da administração necessária.	Ambos	• Gerência de TI. • Segurança da informação. • Prevenção de perdas. • Auditoria interna.	Baixo	Médio

Tabela 1. Modelo Ilustrativo de Avaliação de Riscos de Fraude de TI

Proprietário de Negócios	Riscos de Fraude	Controles	Preventivos ou Detectivos	Monitoramento	Probabilidade	Impacto
TI – CIO	Conflitos de interesses com fornecedores e terceiros.	• Número de linha direta. • Segregação de deveres. • Licitação competitiva. • Comunicação anual para fornecedores e funcionários (tom no topo). • Declaração de ética de negócios. • Comitê de apropriação – despesas de capital. • Lista formal de fornecedores aprovados. • Controles financeiros. • Verificações de histórico.	Ambos	• Comitê de ética. • Recursos humanos. • Prevenção de perdas. • Aquisições. • Finanças. • Auditoria interna.	Baixo	Médio
TI – CIO	Violação de direitos autorais (ex., baixar ou copiar arquivos ilegalmente).	• Conexões <i>peer-to-peer</i> bloqueadas. • Software que identifica programas instalados em estações de trabalho e servidores. • Políticas e procedimentos documentados. • Acesso restrito a mídia física e arquivos de instalação de software.	Ambos	• Operações de TI. • Segurança da informação. • Auditoria interna.	Médio	Médio
TI – CIO	Apropriação indébita de dados da empresa por terceiros (ex., informações de funcionários e clientes, informações confidenciais da empresa).	• Termos do contrato (ex., informações confidenciais, linguagem de privacidade, nenhuma divulgação, devolução de informações confidenciais, direito de auditar). • Arquivos dos clientes de <i>seeding</i>.	Ambos	• Proprietários de negócios. • Segurança da informação. • Auditoria interna.	Baixo	Baixo

Tabela 1. Modelo Ilustrativo de Avaliação de Riscos de Fraude de TI

2.2 Avaliação de Esquemas de Fraude

A seguir estão duas abordagens para avaliar esquemas de fraude da perspectiva do fraudador:¹

- **A abordagem de fraquezas de controle** – Analisa o potencial de fraude examinando os principais controles, determinando quem poderia tirar proveito de uma fraqueza de controle e determinando como ele ou ela poderia contornar um controle que pode não estar funcionando adequadamente.
- **A abordagem dos campos-chave** – Examina o potencial de fraude, considerando os dados que estão sendo inseridos, quais campos podem ser manipulados (e por quem) e qual seria o efeito.

As duas abordagens buscam determinar quem poderia estar cometendo fraude, o que o fraudador poderia estar fazendo e como seriam os sintomas de fraude nos dados. Fazer um *brainstorming* com funcionários das principais áreas de negócios é uma boa técnica para avaliar fraudes e é útil em ambas as abordagens.

2.3 Esquemas de fraude de TI

Conforme a auditoria interna avalia os esforços da organização para concluir uma avaliação abrangente de risco de fraude, é importante que os esquemas de fraude em potencial relacionados à TI sejam identificados e incluídos na avaliação de riscos da empresa. Um dos primeiros passos para realizar essa missão é identificar os indivíduos, dentro da organização, que poderiam concluir a avaliação com eficácia. Os principais participantes a serem considerados incluem a gerência de TI,

¹ Coderre, David G., *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*, John Wiley & Sons, 2009.

gerentes de segurança da informação, gerentes de riscos de TI, gerentes de prevenção de perdas, gerentes de conformidade e outros com habilidades que agreguem valor ao processo. Se a organização não tiver conhecimento interno suficiente de avaliação de fraude, pode considerar cultivar esse talento por meio do desenvolvimento profissional dos funcionários existentes. Em alguns casos, pode ser necessário que a organização vá a uma fonte externa, para obter ajuda para concluir uma avaliação de riscos de fraude de TI com qualidade.

Os seguintes cenários gerais de fraude devem ser considerados e tratados, se aplicáveis à organização.

Acesso a sistemas ou dados para ganho pessoal

Algumas das informações mais valiosas desejadas por indivíduos que cometem uma fraude na área de TI estão na forma de ativos digitais mantidos pela organização. Portanto, é fundamental que as organizações incluam essa área em sua avaliação de riscos de fraude. A maioria das organizações coleta, cria, usa, armazena, divulga e descarta informações que têm valor de mercado para outras pessoas fora da organização. Esses dados podem estar na forma de informações pessoais de funcionários ou clientes, como números de identificação emitidos pelo governo, números de identificação social, números de contas bancárias, números de cartão de crédito, números de contas correntes, números de roteamento bancário e outras informações pessoais. Seja o agressor um indivíduo com acesso autorizado aos dados ou um hacker, essas informações podem ser vendidas a outras pessoas ou usadas para ganhos pessoais, por meio de crimes como roubo de identidade, compras não autorizadas em cartões de crédito roubados, falsificação de cartões de crédito ou roubo ou desvio de dinheiro de uma conta bancária.

Os *insiders*, por terem acesso legítimo às informações, sistemas e redes de suas organizações, representam um risco significativo para os empregadores. Os funcionários que enfrentam problemas financeiros podem ser tentados a usar os sistemas que acessam no trabalho todos os dias para cometer fraudes. Os funcionários motivados por problemas financeiros, ganância, vingança, desejo de obter uma vantagem comercial ou desejo de impressionar um novo empregador podem optar por roubar dados confidenciais, informações proprietárias ou propriedade intelectual de seus empregadores. Além disso, os funcionários técnicos podem usar suas habilidades técnicas para sabotar os sistemas ou redes de seus empregadores, em vingança por eventos negativos relacionados ao trabalho.²

Os exemplos a seguir ilustram como o acesso inadequado a sistemas ou dados resultou em ganho pessoal ou destruição do sistema.

- Uma funcionária do departamento de folha de pagamento de uma empresa de telecomunicações assumiu um novo cargo no departamento, no qual ela não precisaria mais ter acesso privilegiado às contas de folha de pagamento. Ao mudar de cargo, os direitos de acesso da funcionária às contas da folha de pagamento foram mantidos inalterados. Um associado disse a ela que estava iniciando uma empresa de serviços financeiros e precisava de algumas informações de contato. Usando os direitos de acesso privilegiados que ela reteve, a funcionária forneceu informações confidenciais de 1.500 funcionários da empresa, incluindo números de contas 401k, números de conta de cartão de crédito e números de seguro social, que ele usou, então, para mais de 100 casos de roubo de identidade. As ações dos criminosos causaram mais de US\$ 1 milhão em danos à empresa e seus funcionários.³
- Um analista de banco de dados de uma grande empresa de autorização de cheques e processamento de cartões de crédito excedeu seu acesso autorizado ao computador. O funcionário usou seu acesso ao computador para roubar as informações de consumo de 8,4 milhões de pessoas. As informações roubadas incluíam nomes e endereços, informações sobre contas bancárias e informações sobre cartões de crédito e débito. Ele vendeu os dados para operadores de telemarketing durante um período de cinco anos. Um juiz distrital dos EUA condenou-o a 57 meses de prisão e US\$ 3,2 milhões em restituição por conspiração e fraude informática.⁴
- Um consultor de TI estava trabalhando sob contrato para uma empresa de plataformas de petróleo *off-shore*. Depois que a empresa se recusou a oferecer a ele um emprego permanente, ele acessou ilegalmente os sistemas da empresa e causou danos ao prejudicar a integridade e a disponibilidade dos dados. Ele foi indiciado em acusações federais, que têm pena máxima legal de 10 anos em prisão federal.⁵

² “The, Big Picture, of Insider IT Sabotage Across U.S. Critical Infrastructures.” Carnegie Mellon, maio de 2008.

³ “Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector.” U.S. Secret Service e CERT Coordination Center/SEI, janeiro de 2008.

⁴ Website do U.S. Department of Justice, Computer Crime and Intellectual Property Section, <http://usdoj.gov/criminal/cybercrime>, 2009.

⁵ Website do U.S. Department of Justice, Computer Crime and Intellectual Property Section, <http://usdoj.gov/criminal/cybercrime>, 2009.

Outros possíveis esquemas de fraude de TI nessa categoria incluem copiar e distribuir software proprietário para ganho pessoal, e acessar e usar informações confidenciais da empresa, como relatórios financeiros, informações dos fornecedores ou planos de negócios estratégicos para ganho pessoal. Por exemplo, um funcionário descontente ou demitido pode copiar e distribuir ou vender ilegalmente software proprietário. O criminoso pode, então, tentar cobrir seus rastros, alterando ou excluindo os logs de auditoria e alterando outros dispositivos de monitoramento usados para detectar problemas.

Alterações em Programas ou Dados do Sistema para Ganho Pessoal

Se a organização tiver falhas de controle ou fraquezas no ciclo de vida de desenvolvimento de sistemas, existem oportunidades para fraudes. Os exemplos na Tabela 2 – Fraude no Desenvolvimento de Sistemas⁶ ajudam a demonstrar como a fraude pode ocorrer em cada uma das fases de desenvolvimento do sistema.

⁶ “Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector.” U.S. Secret Service e CERT Coordination Center/SEI, janeiro de 2008.

Fase	Fraude	Descuido
Fase de Definição dos Requisitos	195 carteiras de motoristas ilegítimas são criadas e vendidas por um oficial de comunicações da polícia, que acidentalmente descobre que pode criá-las.	- Requisitos de autenticação e controle de acesso baseados em funções mal definidos. - Requisitos de segurança mal definidos para processos de negócios automatizados. - Falta de segregação de deveres.
Fase de Design do Sistema	- Uma função especial para agilizar o tratamento de casos permite que dois assistentes embolsem US\$ 32.000 em propinas. - Um funcionário percebe que não há supervisão no sistema e nos processos de negócios de sua empresa, então, trabalha com o crime organizado para entrar e lucrar US\$ 20 milhões em falsos pedidos de seguro de saúde.	- Atenção insuficiente aos detalhes de segurança de processos automatizados do fluxo de trabalho. - Falta de consideração pelas vulnerabilidades de segurança representadas pelas sobrescritas autorizadas do sistema.
Fase de Implementação do Sistema	Um ex-desenvolvedor Web de 18 anos usa <i>backdoors</i> que inseriu em seu código para acessar a rede de sua antiga empresa, enviar spam a seus clientes, alterar seus aplicativos e, por fim, acabar com o negócio da empresa.	Falta de revisões no código.
Fase de Desenvolvimento do Sistema	- Um técnico de informática usa seu acesso irrestrito aos sistemas dos clientes para implantar um vírus em suas redes, o que paralisa os sistemas dos clientes. - Um engenheiro de software deliberadamente não cria documentação ou backup para seu código-fonte e, em seguida, exclui a única cópia do código-fonte quando o sistema está em produção.	- Falta de cumprimento das práticas de documentação e procedimentos de backup. - Acesso irrestrito aos sistemas de todos os clientes.
Fase de Manutenção do Sistema	- Um operador de moeda estrangeira encobre perdas de US\$ 691 milhões ao longo de um período de cinco anos, fazendo alterações não autorizadas no código-fonte. - Uma bomba lógica não é detectada por seis meses, antes de finalmente executar uma exclusão em massa dos dados de uma empresa de telecomunicações.	- Falta de revisões no código. - Acesso do usuário final ao código-fonte. - Processos ineficazes de backup, que amplificaram o impacto da exclusão em massa de dados.

Figura 2. Fraude no Desenvolvimento de Sistemas

Outras vulnerabilidades de fraude de TI que devem ser consideradas durante a avaliação de risco incluem:

- Cobrança fictícia por serviços ou apropriação indébita de dados confidenciais de funcionários, clientes ou empresas para ganho pessoal por parte de um contratado independente ou programador *on-shore* ou *off-shore*.
- Violação de direitos autorais e perda de propriedade intelectual quando funcionários ou contratados copiam ou baixam arquivos ilegalmente.
- Apropriação indébita de dados da empresa por parte de prestadores de serviços terceirizados, que processam informações de funcionários e/ou clientes ou outras informações confidenciais da empresa.

A seguir estão alguns exemplos de práticas recomendadas para lidar com os riscos de fraude de TI.

- Fazer avaliações periódicas dos riscos de fraude de TI em toda a empresa.
- Instituir um treinamento periódico de segurança e conscientização de fraude para todos os funcionários.
- Reforçar a segregação de deveres.
- Restringir o acesso a sistemas e dados com base na necessidade comercial de saber.
- Implementar políticas e práticas rigorosas de gestão de identidades e senhas.
- Registrar, monitorar e auditar as ações dos funcionários na rede.
- Ter cuidado extra com os administradores do sistema e usuários privilegiados.
- Usar camadas de defesa contra intrusões na rede.
- Desenvolver um plano eficaz de resposta a incidentes e montar uma equipe de resposta a incidentes.
- Desativar o acesso ao computador após a rescisão do contrato de trabalho do funcionário.
- Coletar e salvar dados forenses para uso em investigações.
- Permitir um processo seguro de backup e recuperação.
- Implementar bons programas de gestão de vulnerabilidades.

3. Detecção de Fraude Usando a Análise de Dados

O objetivo deste capítulo é auxiliar os auditores internos a assumirem um papel proativo no tratamento de fraudes, usando técnicas de análise de dados. O capítulo aborda detalhadamente por que a tecnologia de análise de dados é importante, técnicas analíticas específicas comprovadas como altamente eficazes, tipos típicos de testes de fraude, a importância de analisar populações de dados completas, estratégias de programas de detecção de fraudes e análise de dados usando fontes internas e externas de dados.

3.1 Por Que Usar a Análise de Dados para Detecção de Fraudes?

A tecnologia de análise de dados permite que os auditores e outros examinadores de fraudes analisem dados transacionais para obter insights sobre a eficácia operacional dos controles internos e para identificar indicadores de riscos de fraude ou atividades fraudulentas reais. Seja para revisar registros de folha de pagamento para funcionários fictícios ou transações de contas a pagar de faturas duplicadas, a tecnologia da análise de dados pode ajudar os auditores internos a lidar com riscos de fraude dentro da organização.

Para testar e monitorar os controles internos com eficiência, as organizações devem analisar todas as transações relevantes em relação aos parâmetros de controle, em todos os sistemas e em todos os aplicativos. Examinar as transações no nível da fonte ajuda a garantir a integridade e a precisão das informações.

Os principais fatores que determinam se o auditor pode confiar nos dados ou se mais testes de integridade de dados são necessários incluem:

- A familiaridade do auditor com os dados de origem.
- Os controles gerais e de aplicativos.
- A confiança depositada nos dados.
- A existência de evidências corroborantes.

O primeiro teste dos dados deve ser verificar sua integralidade e integridade. A integralidade e integridade dos dados são de suma importância ao lidar com possíveis fraudes, porque registros ausentes ou campos em branco podem falsamente indicar fraude ou fazer com que possíveis fraudes passem despercebidas. Em seguida, testes adicionais devem ser realizados para contribuir para o entendimento do auditor sobre os dados e para buscar sintomas de fraude nos dados.⁷

3.2 Técnicas Analíticas para Detecção de Fraude

Várias técnicas analíticas específicas foram comprovadas como altamente eficazes para a detecção de fraudes. Os

departamentos de auditoria devem considerar essas diversas técnicas ao avaliar o uso da tecnologia na detecção de fraudes:

- Cálculo de parâmetros estatísticos (ex., médias, desvios-padrão, valores mais altos e mais baixos) – para identificar transações periféricas que possam ser indicativas de atividade fraudulenta.
- Classificação – para encontrar padrões e associações entre grupos de elementos de dados.
- Estratificação de valores numéricos – para identificar valores incomuns (ou seja, excessivamente altos ou baixos).
- Análise digital usando a Lei de Benford – para identificar ocorrências estatisticamente improváveis de dígitos específicos em conjuntos de dados que ocorrem aleatoriamente.
- Unir diferentes fontes de dados – para identificar valores de correspondência inadequados, como nomes, endereços e números de conta em sistemas diferentes.
- Teste de duplicata – para identificar duplicações simples e/ou complexas de transações comerciais, como pagamentos, folha de pagamento, reclamações ou itens de linha do relatório de despesas.
- Teste de lacuna – para identificar números ausentes em dados sequenciais.
- Soma dos valores numéricos – para verificar os totais de controle que possam ter sido falsificados.
- Validar as datas da entrada de dados – para identificar postagens ou tempos de entrada de dados inadequados ou suspeitos.

De acordo com um *white paper*⁸ de 2008 da ACL Services Ltd., para maximizar a eficácia da análise de dados na detecção de fraudes, a tecnologia empregada deve permitir que os auditores:

- Comparem dados e transações de diversos sistemas de TI (e abordem lacunas de controle que existem frequentemente dentro e entre sistemas).
- Trabalhem com um conjunto abrangente de indicadores de fraude.
- Analisem todas as transações dentro da área de destino.
- Realizem os testes de detecção de fraude em uma base programada e forneçam notificações tempestivas de tendências, padrões e exceções.

3.3 Tipos Típicos de Testes de Fraude

As técnicas de análise de dados descritas anteriormente podem ser aplicadas a um grande número de áreas dentro de uma organização. A priorização de onde procurar precisa ser feita em conjunto com um processo de avaliação de riscos de fraude. A Tabela 3 – Testes de Detecção de Fraudes oferece exemplos de alguns dos testes de detecção de fraudes que podem ser realizados usando a análise de dados.

⁷ Coderre, David G. *Fraud Analysis Techniques Using ACL*. John Wiley & Sons, 2009.

⁸ “Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection.” ACL Services Ltd., 2008.

GTAG — Detecção de Fraude Usando a Análise de Dados

Tipo de Fraude	Testes Usados para Descobrir Esta Fraude
Fornecedores fictícios	• Executar verificações para descobrir caixas postais usadas como endereços e para encontrar correspondências entre endereços e/ou números de telefone de fornecedores e funcionários. • Estar alerta a fornecedores com nomes semelhantes ou mais de um fornecedor com o mesmo endereço e número de telefone.
Notas alteradas	• Procurar por duplicatas. • Verificar os valores da fatura que não correspondam aos contratos ou valores do pedido.
Licitação fraudulenta	• Resumir o valor do contrato por fornecedor e comparar os resumos dos fornecedores de diversos anos, para determinar se um único fornecedor está ganhando a maioria das licitações. • Calcular os dias entre o fechamento das ofertas e a data de submissão do contrato pelo fornecedor, para verificar se o último licitante ganhou o contrato de forma consistente.
Bens não recebidos	• Procurar quantidades de compra que não correspondam às quantidades do contrato. • Verificar se os níveis de estoque estão mudando em relação à suposta entrega de mercadorias.
Notas duplicadas	• Analisar números duplicados de faturas, datas duplicadas e valores duplicados de faturas.
Preços inflacionados	• Comparar os preços entre os fornecedores, para ver se os preços de um determinado fornecedor são excessivamente altos.
Quantidades compradas em excesso	• Revisar os aumentos inexplicáveis no estoque. • Determinar se as quantidades de compra de matérias-primas são apropriadas para o nível de produção. • Verificar se os aumentos nas quantidades encomendadas se comparam de maneira semelhante aos contratos ou anos anteriores, ou a outras fábricas.
Pagamentos duplicados	• Procurar números de fatura idênticos e valores de pagamento. • Verificar pedidos recorrentes de reembolso para faturas pagas duas vezes.
Cópias em papel carbono	• Procurar duplicatas em todos os cheques da empresa que tenham sido compensados. • Realizar uma segunda busca por lacunas nos números dos cheques.
Números de série duplicados	• Determinar se o equipamento de alto valor que uma empresa já possui está sendo recomprado, verificando números de série duplicados e o envolvimento da mesma equipe nos processos de compra e envio.
Fraude de folha de pagamentos	• Verificar se um empregado demitido ainda está na folha de pagamento, comparando a data de término com o período de pagamento coberto pelo cheque e extrair todas as transações de pagamento com data de partida anterior à data do período de pagamento atual.
Contas a pagar	• Encontrar transações que não correspondam aos valores do contrato, vinculando os arquivos de contas a pagar aos arquivos de contrato e inventário, e examinando a data do contrato, preço, quantidade solicitada, quantidade do recibo do inventário, quantidade na fatura e valor do pagamento por contrato.

Fonte: *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*,⁹ by David Coderre.

Tabela 3. Testes de Detecção de Fraudes

⁹ Coderre, David G. *Computer Aided Fraud Prevention and Detection: A Step-by-Step Guide*. John Wiley & Sons, 2009.

Para testes analíticos que dependam do acesso e uso de informações pessoais e/ou sensíveis, os auditores devem ter o devido cuidado em salvaguardar essas informações. As organizações também devem garantir que uma avaliação de riscos de privacidade seja realizada para os casos em que o uso de informações pessoais seja restrito pela legislação local. Para obter informações adicionais sobre esse tópico, consulte o GTAG 5 do The IIA: *Managing and Auditing Privacy Risks*.¹⁰

3.4 Analisando Populações de Dados Completos

Para que os programas de detecção de fraudes sejam eficazes, as técnicas de detecção de fraudes listadas na seção anterior devem ser executadas em relação às populações de dados completas. Embora os dados de amostragem sejam uma abordagem de auditoria válida e eficaz, eles não são necessariamente apropriados para fins de detecção de fraudes. Quando apenas dados parciais são testados, é provável que várias violações de controle e transações suspeitas sejam perdidas; o impacto de falhas de controle pode não ser quantificado totalmente; e anomalias menores podem ser perdidas. Muitas vezes, são essas pequenas anomalias que apontam para pontos fracos que possam ser explorados, causando uma violação material.

A análise dos dados em comparação com as populações de dados completas fornece um quadro mais completo de possíveis anomalias. A amostragem aleatória é mais eficaz para identificar problemas que são relativamente consistentes em toda a população de dados; transações fraudulentas, por natureza, não ocorrem aleatoriamente.

3.5 Prevenção de Fraudes e Estratégias do Programa de Detecção

Em vez de adotar uma abordagem reativa à detecção de fraudes, confiando apenas em pistas e programas de denúncia, as organizações devem adotar uma abordagem proativa para combater a fraude. Sua abordagem deve incluir uma avaliação, por parte da auditoria interna, da eficácia operacional dos controles internos, juntamente com uma análise dos dados no nível de transação, em busca de indicadores específicos de fraude.

Um programa de prevenção e detecção de fraudes deve incorporar um espectro de análise dos dados transacionais – variando de *ad hoc*, para repetitivo, para contínuo. Com base nos principais indicadores de riscos, testes *ad hoc* identificarão áreas para investigação adicional. Se o teste inicial revelar deficiências de controle ou suspeita de incidência de fraude, testes repetitivos ou análises contínuas devem ser considerados. A análise de dados transacionais é uma das formas mais eficientes e eficazes de detectar fraudes em uma organização, e as organizações

podem determinar a implantação ao longo do espectro de análise, com base nas áreas de riscos de fraude.¹¹

Segundo o relatório *Fraud Risk Management* da KPMG, “ao contrário das análises retrospectivas, o monitoramento contínuo de transações permite que a organização identifique transações potencialmente fraudulentas, por exemplo, diariamente, semanalmente ou mensalmente. As organizações frequentemente usam esforços contínuos de monitoramento para se concentrar em pequenas faixas de transações ou em áreas que apresentem riscos particularmente fortes”.¹²

Ao aplicar a tecnologia de análise de dados em uma base contínua ou repetitiva – seja como uma auditoria contínua ou uma iniciativa de monitoramento contínuo –, as organizações podem detectar fraudes mais cedo e reduzir a probabilidade de uma perda maior. Para obter informações adicionais sobre a relação entre auditoria contínua e monitoramento contínuo, consulte o GTAG 3 do The IIA: *Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment*.¹³

3.6 Analisando Dados Usando Fontes de Dados Internas e Externas

Para que a análise de dados seja eficaz na detecção de fraudes, é necessário integrar dados de diversas fontes, incluindo financeiras, não financeiras, internas e externas. O uso dessas diversas fontes de dados fornece uma visão mais abrangente da organização a partir de uma perspectiva de fraude. A Tabela 4 – Fontes de Dados Diversas ilustra essa visão abrangente.

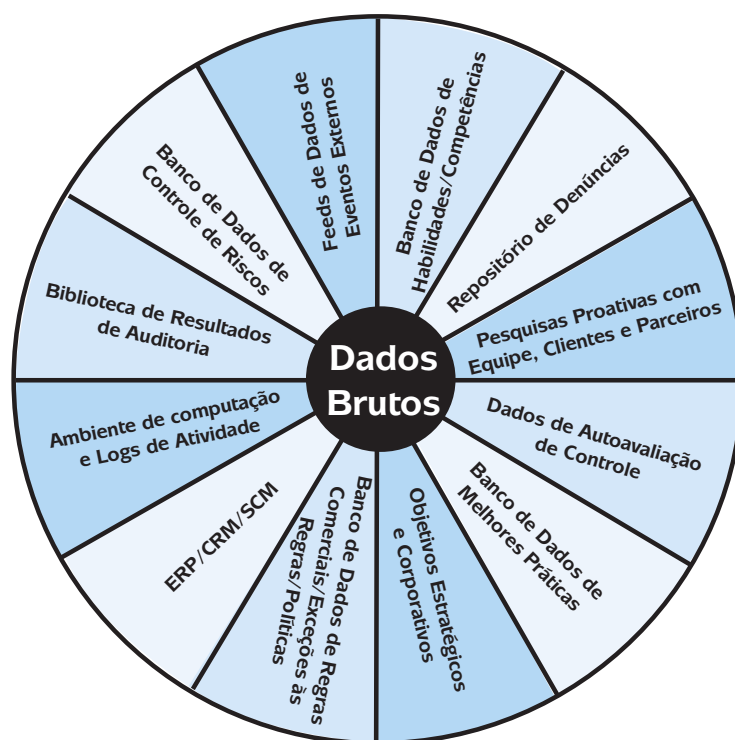
As organizações devem usar essas e outras fontes de dados para conduzir uma análise de dados de fraude, incluindo o processo integrado de quatro etapas ilustrado na Tabela 5 – Análise de Dados de Fraude.

¹⁰ GTAG 5: *Managing and Auditing Privacy Risks*. The Institute of Internal Auditors, 2006.

¹¹ “Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection.” ACL Services Ltd., 2008.

¹² “Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response.” KPMG International, 2006.

¹³ GTAG 3: *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*. The Institute of Internal Auditors, 2005.



Fonte: *The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*¹⁴

Tabela 4. Fontes Diversas de Dados

¹⁴ Lanza, Richard B. Brooks, Dean; e Goldman, Mort. *The Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*. Ekaros Publishing, 2008.

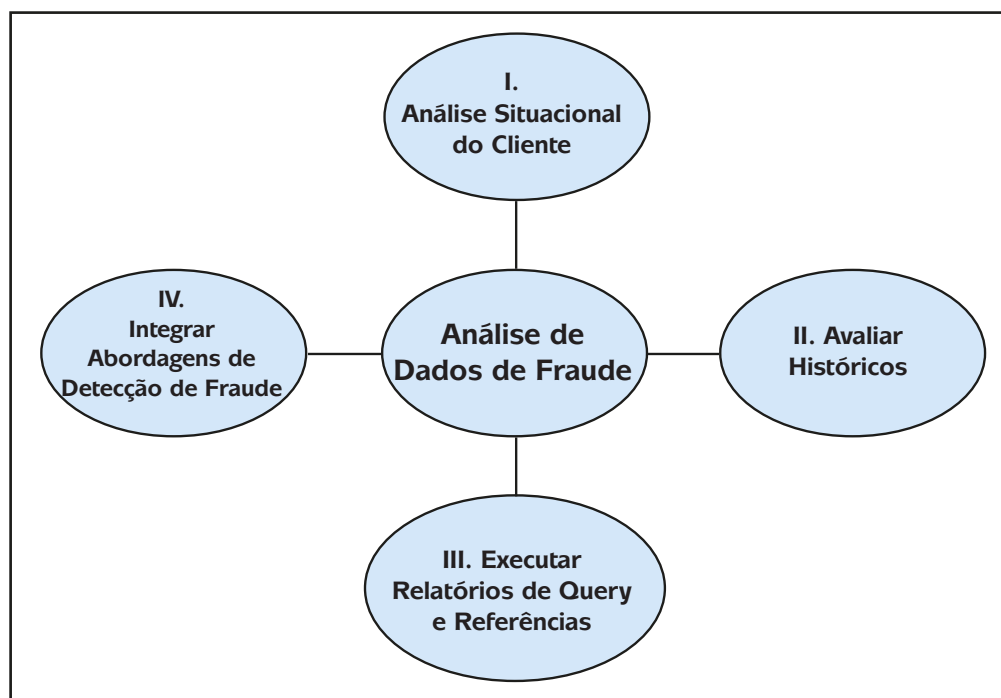


Tabela 5. Análise de Dados de Fraude

I. Faça uma Análise Situacional

Identifique os principais riscos de fraude a partir de uma perspectiva de impacto e probabilidade para uma organização específica. Os controles internos usados para minimizar os riscos de fraude devem ser levados em conta, assim como os planos para pesquisar os resultados de uma avaliação de riscos de fraude. Consulte o Capítulo 2 para obter mais informações sobre a realização de uma avaliação de riscos para procurar fraudes.

II. Avalie os Históricos das Principais Partes Associadas às Transações

Normalmente, as pesquisas de histórico são concluídas apenas para funcionários ou candidatos a emprego. As organizações também devem considerar o uso de bancos de dados da Internet para realizar pesquisas de histórico sobre fornecedores, clientes e parceiros de negócios associados às transações em áreas de alto risco de fraude. Por exemplo, o processo de aquisição pode ser visto como um alto risco de atividade fraudulenta em uma organização. Com isso em mente, a organização pode optar por analisar os fornecedores que são grandes (em termos de dólares), aqueles que aumentaram de tamanho nos últimos anos ou aqueles que estão aparecendo em uma variedade de relatórios de possíveis atividades de fraude.

A maioria dos países tem várias fontes e listas de dados do governo e do setor disponíveis que podem ajudar as organizações a identificar empresas barradas, sancionadas ou sob vigilância. O *Excluded Parties List System* (www.epls.gov), dos Estados Unidos, fornece informações sobre as partes que estão excluídas do recebimento de contratos federais e certos benefícios e assistência financeira federais. Os bancos de dados de informações de empresas, como o Dun & Bradstreet e o Equifax, também podem ser usados para identificar problemas comerciais que afetam as empresas, como ações judiciais pendentes e dificuldades financeiras. Essas são fontes externas de dados úteis de se considerar, desde que a organização tenha identificado objetivos e resultados claros para seu uso na detecção de fraudes. A lista a seguir oferece exemplos do tipo de informação que pode ser obtida dessas fontes e usada para ajudar a avaliar a natureza possivelmente fraudulenta de uma empresa.

- Endereço da empresa e/ou número de telefone inválido.
- Conflitos de interesses com os funcionários atuais.

- Número de identificação fiscal inválido.
- Incapacidade de encontrar evidências da existência da empresa em qualquer uma das fontes de dados externas.
- Funcionários que se apresentam como fornecedores.
- Relações de três vias entre os funcionários, seus parentes próximos e fornecedores.
- Tipo arriscado de empresa (ex., empresa individual pode ser mais arriscada).
- Empresa recém-criada.
- Questões jurídicas anteriores ou outras questões especiais.

O uso de bancos de dados externos ajuda as organizações a obter uma imagem mais clara dos parceiros de negócios sob a perspectiva de seu potencial para cometer fraudes.

III. Execute uma Variedade de Consultas e Calcule Estatísticas de Linha de Base

Com base nos riscos de fraude identificados da empresa, as consultas podem ser executadas por auditores internos e os resultados podem ser combinados para identificar parceiros de negócios, fornecedores, departamentos da empresa, funcionários e até transações específicas que pareçam ser fraudulentas. As estatísticas de linha de base podem ser calculadas para parceiros de negócios, departamentos da empresa, funcionários, horário e outras categorias. Então, qualquer atividade adicional estaria relacionada à linha de base, para identificar possíveis exceções ou alertas que exigiriam análises adicionais.

Uma ferramenta útil para gerar ideias de relatórios é o estudo da The IIA Research Foundation, *Proactively Detecting Fraud Using Computer Assisted Audit Reports*.¹⁵

Um exemplo desta publicação relacionado a esquemas de faturamento é mencionado abaixo.

¹⁵ Lanza, Richard B., "Proactively Detecting Fraud Using Computer Assisted Audit Reports," The IIA Research Foundation, 2003.

ESQUEMAS DE FATURAMENTO

Os esquemas de faturamento ocorrem quando um fraudador envia faturas de bens ou serviços fictícios, faturas inflacionadas ou faturas de compras pessoais, solicitando que a organização vítima emita um pagamento. Existem três subcategorias de esquemas de faturamento:

- Empresa Fantasma – Uma organização falsa é criada nos livros da empresa, para uso no pagamento de faturas fictícias.
- Fornecedor Não Cúmplice – O pagamento de um fornecedor é feito indevidamente, de forma intencional, para efetuar um pagamento fictício ao funcionário.
- Compras Pessoais – Compras pessoais são feitas usando contas da empresa, como um cartão de compras da empresa.

Procedimento de Teste	Detalhe e Análise do Teste	Arquivo(s) de Dados
Identificar pagamentos duplicados com base em diversos meios.	Testes de pagamentos duplicados podem ser feitos quanto ao fornecedor, o número da fatura e o valor. Testes mais complicados podem identificar casos em que a mesma fatura e quantia tenham sido pagas, mas o pagamento tenha sido feito para dois fornecedores diferentes.	• Pagamento da fatura
Resumir as notas de débito por fornecedor, emissor e tipo.	Tendências de notas de débito que pareçam não usuais devem ser investigadas, pois podem indicar tentativas de encobrir pagamentos não autorizados.	• Pagamento da fatura
Identificar verificações manuais e resumir por fornecedor e emissor.	As verificações manuais são mais propensas a abuso e, portanto, devem ser analisadas, especialmente se um funcionário em particular estiver fazendo a maioria das verificações manuais.	• Verificação de caixa
Encontrar todas as compras sem pedidos de compras e fazer um resumo por fornecedor e emissor.	As compras sem pedidos de compra são mais propensas a abusos e, portanto, devem ser analisadas, especialmente se as faturas não tiverem pedidos de compra correspondentes.	• Pagamento da fatura
Comparar o arquivo mestre do fornecedor com o arquivo de fatura de contas a pagar.	Identificar pagamentos para um fornecedor potencialmente não aprovado, associando o arquivo do fornecedor ao arquivo da fatura ou ao número do fornecedor. Isso deve ser feito com base na “não correspondência” – de modo que apenas os números de fornecedor na fatura que <i>não</i> aparecem no arquivo do fornecedor sejam exibidos.	• Arquivo mestre do fornecedor • Pagamento da fatura
Extrair fornecedores sem telefone ou número de identificação fiscal.	Fornecedores sem essa informação são mais propensos ao abuso e devem ser analisados.	• Arquivo mestre do fornecedor

Ao produzir estatísticas de consulta e de linha de base, os auditores devem usar as perguntas clássicas dos “Cinco W”: quem, o quê, por que, onde e quando (*who, what, why, where* e *when*). Muitos profissionais usam essa abordagem para obter uma perspectiva holística da situação e das circunstâncias completas. A utilização da abordagem dos “Cinco W” para revisar os lançamentos, conforme ilustrada abaixo, provoca uma maior probabilidade de detectar entradas de razão geral incomuns ou fraudulentas.¹⁶

Quem fez a entrada no diário?

- Identificar as entradas inseridas no diário por funcionários não autorizados ou usuários restritos.

Qual foi a natureza da entrada no diário?

- Identificar lançamentos contábeis manuais ou fora do padrão (em vez de lançamentos padrão ou automatizados, como aqueles de um lançamento contábil de contas a pagar).
- Identificar lançamentos contábeis por conta de razão geral, para identificar sequências de contas repetitivas e únicas (com base nos primeiros 10 lançamentos de conta de débito e crédito).

Quando a entrada foi inserida no diário?

- Identificar os lançamentos feitos nos finais de semana e feriados.
- Classificar o processamento de créditos e débitos lançados no diário por dia, mês e ano.
- Resumir o processamento de créditos e débitos lançados no diário por dia, mês e ano.

Por que há atividade incomum relacionada ao lançamento no diário?

- Filtrar transações do razão geral (débito ou crédito) que excedam os valores médios dessa conta por uma porcentagem especificada. (Cinco vezes a média é um bom ponto de partida.)
- Identificar lançamentos que contenham linguagem questionável em suas descrições, como os termos “*plug*”, “*balance*” e “*net to zero*”.
- Identificar lançamentos que não resultem em zero (débitos menos créditos).

¹⁶ Lanza, Richard B. e Gilbet, Scott. “Maximizing Journal Entry Testing Through Automation.” ITAudit, 2007.

IV. Integrar as Abordagens Anteriores em uma Análise Consolidada

Combinando os resultados dos procedimentos descritos na Etapa III, anteriormente, e usando a metodologia de pontuação, as organizações podem desenvolver uma lista direcionada ao parceiro de negócios, departamento, funcionário e/ou nível de transação. Ao desenvolver a lista, o nível de especificidade desejado pela empresa, além dos planos da empresa para pesquisar qualquer atividade incomum, devem ser considerados.

Uma maneira de pontuar a atividade é atribuir um ponto a cada resultado que contenha um parceiro de negócios/transação e, em seguida, atribuir um peso a essa pontuação com base na quantidade de processamento associada ao parceiro de negócios/transação em particular. Isso pode ser explicado melhor usando o exemplo de razão geral anterior e marcando a atividade de acordo, da seguinte maneira:

Passo 1 – Uma pontuação numérica de um (1) foi dada para cada entrada no diário que apareceu em cada um dos seguintes testes de auditoria.

1. Entradas de diário não padrão ou manuais.
2. Lançamentos de diário feitos para contas suspensas, agrupados pela pessoa que fez o lançamento e agrupados por números de contas correspondentes.
3. Valores de transações do razão geral que excedam os valores médios para essa conta por uma porcentagem especificada.
4. Entradas de diário que contenham linguagem questionável em suas descrições.
5. Entradas de diário que não resultem em zero.

Passo 2 – As pontuações do Passo 1 foram adicionadas, para criar uma pontuação numérica total. Por exemplo, uma entrada de diário que atendia às condições dos testes de auditoria 1, 3 e 6 na Etapa 1 recebeu uma pontuação numérica de três.

Passo 3 – A pontuação numérica total de cada entrada de diário do Passo 2 foi multiplicada pela quantidade dos débitos dos lançamentos em diário correspondentes, para criar uma pontuação ponderada. Por exemplo, um lançamento contábil com uma pontuação numérica de três no Passo 2, com débitos de conta totalizando US\$ 100.000, tem uma pontuação ponderada de US\$ 300.000 (3x \$ 100.000).

Passo 4 – As entradas em diário foram classificadas pela pontuação numérica total, conforme o Passo 2 acima, e as 20 principais entradas em diário com pontuação numérica foram detalhadas em um relatório. As entradas no diário foram então classificadas pela pontuação ponderada, conforme o Passo 3 acima, e os 20 principais lançamentos ponderados foram extraídos para um relatório.

Embora cada relatório de entrada contábil manual possa ser revisado isoladamente, é mais eficaz revisá-los em conjunto, de

modo que o auditor interno possa se concentrar nos lançamentos contábeis mais prováveis ou incomuns. Assim, se um determinado lançamento contábil apareceu em muitos relatórios suspeitos, é mais provável que seja incomum ou associado a uma sobrescrita inapropriada da administração.

4. O Papel do CAE em Lidar com a Fraude de TI

O objetivo deste capítulo é fornecer ao CAE orientações sobre a comunicação com o comitê de auditoria sobre os riscos de fraude de TI, e sobre fazer perguntas regularmente para ajudar a entender melhor os riscos de fraude de TI e o papel da auditoria interna na organização. Ideias específicas estão incluídas sobre os tipos de informações relacionadas à fraude de TI que devem ser consideradas para compartilhamento com o comitê de auditoria. O capítulo também inclui vinte perguntas sobre a fraude de TI e dicas sobre o que incluir em uma política de investigação de fraudes, para ajudar os auditores internos a entender melhor como a organização lida com os riscos de fraude.

4.1 O Comitê de Auditoria

O relacionamento entre o CAE e o comitê de auditoria deve incluir o reporte de atividades de auditoria interna relacionadas aos riscos de fraude de TI e às avaliações de riscos de fraude de TI. Manter a conscientização sobre o que está acontecendo dentro da organização e seu setor específico aumenta a capacidade do CAE de lidar com os riscos de fraude de TI junto com o comitê de auditoria.

O que exatamente os CAEs discutem com seus comitês de auditoria, no que tange à fraude de TI ou fraudes possibilitadas pela tecnologia? Na maioria dos casos, não é diferente das atualizações habituais para a alta administração e para o comitê de auditoria sobre fraudes. O Guia Prático do The IIA, *Internal Auditing and Fraud*, fornece informações sobre como se comunicar com o conselho. Por outro lado, o comitê de auditoria pode exigir uma explicação mais detalhada da tecnologia ou da área de TI afetada, para melhor compreender o impacto e o risco para a organização. Portanto, o CAE deve estar familiarizado – e ser capaz de comunicar ao comitê de auditoria – como a organização gerencia e controla os recursos críticos de TI e o papel que a auditoria interna desempenha nessa área.

O CAE pode discutir os seguintes tópicos de fraude de TI com o comitê de auditoria:

- O papel da auditoria interna nas investigações de fraude de TI.
- Todas as auditorias de fraude realizadas na área de TI.
- O processo realizado para a avaliação de riscos de fraude de TI.
- Fraudes de TI ou conflitos de interesses, e os resultados dos programas de monitoramento referentes à conformidade com a lei, código de conduta e/ou ética.
- A estrutura organizacional da atividade de auditoria interna, no que se refere à abordagem de fraude de TI.
- A coordenação da atividade de auditoria de fraude de TI com auditores externos.
- A avaliação geral do ambiente de controle de fraudes da organização na TI.

- Medidas de produtividade e orçamentárias para as atividades de fraude de TI da auditoria interna.
- *Benchmarking* das atividades de fraude de TI da auditoria interna em relação a outras empresas.

4.2 Vinte Perguntas que o CAE Deveria Perguntar Sobre Fraude

O CAE nunca deve relutar em fazer perguntas sobre fraude. Ter conversas tempestivas e apropriadas sobre fraude com todos os níveis da organização, incluindo o comitê de auditoria, demonstra que a atividade de auditoria interna está assumindo um papel proativo nessa área. Algumas das muitas perguntas que o CAE deve fazer regularmente sobre a fraude de TI incluem:

1. A organização possui uma estrutura de governança de fraude que atribua responsabilidades pelas investigações de fraude de TI?
2. A organização possui uma política de resposta a incidentes de fraude de TI? (Consulte O Que Incluir em uma Política de Investigação de Fraude, a seguir, para mais informações.)
3. A organização identificou leis e regulamentos relacionados à fraude de TI nas jurisdições onde faz negócios?
4. O programa de gestão de fraudes de TI da organização inclui a coordenação com a auditoria interna?
5. A organização possui um canal de denúncias de fraude que notifique os indivíduos apropriados sobre preocupações com fraudes envolvendo os recursos de TI?
6. O estatuto de auditoria menciona as funções e responsabilidades dos auditores internos em relação à fraude de TI?
7. A responsabilidade pela detecção, prevenção, resposta e conscientização de fraudes de TI foi atribuída dentro da organização?
8. A administração e o CAE informam o comitê de auditoria sobre fraudes de TI?
9. A administração promove a conscientização e o treinamento de fraude de TI dentro da organização?
10. A administração conduz avaliações de riscos de fraude de TI e inclui a auditoria interna no processo de avaliação?
11. Os resultados das avaliações de riscos de fraude de TI são implementados no processo de planejamento de auditoria?
12. Os programas periódicos de conscientização e treinamento de fraude de TI são fornecidos aos auditores internos?
13. Existem ferramentas automatizadas disponíveis para os responsáveis por prevenir, detectar e investigar fraudes de TI?
14. A administração identificou os tipos de riscos potenciais de fraude de TI em suas áreas de responsabilidade?
15. A administração e o CAE sabem onde obter orientação sobre fraudes de TI por parte de organizações profissionais?
16. A administração e os auditores internos conhecem suas responsabilidades profissionais relacionadas à fraude de TI?
17. A administração incorporou controles apropriados para prevenir, detectar e investigar fraudes de TI?

18. A administração possui os conjuntos de habilidades apropriados para realizar investigações de fraude de TI?
19. A administração e a auditoria interna avaliam periodicamente a eficácia e a eficiência dos controles de fraude de TI?
20. Os papéis de trabalho de investigação de fraude de TI e os documentos de apoio são devidamente protegidos e retidos?

O Que Incluir em uma Política de Investigação de Fraude

1. Como e quando iniciar uma investigação de fraude.
2. Requisitos de documentação para a investigação de fraude.
3. Como selecionar a equipe de investigação.
4. O processo para adicionar especialistas à equipe.
5. Como analisar, avaliar e mitigar os controles internos.
6. Como e quando escalar as investigações.
7. Consistência e uniformidade, para garantir que todas as ocorrências sejam tratadas da mesma forma.
8. Orientação sobre até que ponto a organização está disposta a realizar uma investigação.
9. Canais de comunicação para usar antes, durante e depois da investigação.
10. Diretrizes sobre a extensão dos esforços de recuperação a serem realizados.

Referências e Recursos

Institutos e Associações:

American Institute of Certified Public Accountants
(AICPA) – www.aicpa.org

Association of Certified Fraud Examiners (ACFE) – www.acfe.org

The Institute of Internal Auditors (IIA) – www.theiia.org

Leis e Regulamentos Internacionais Relativos à Fraude:

Austrália – Corporate Law Economic Reform Program Act de 2004

Canadá – Código Criminal

União Europeia – Financial Services Action Plan

Reino Unido – Companies Act de 2004

Estados Unidos – USA PATRIOT Act, Foreign Corrupt Practices
Act, U.S. Sarbanes-Oxley Act de 2002

Outras Referências:

“2008 Report to the Nation on Occupational Fraud & Abuse,”
Association of Certified Fraud Examiners, 2008.

“Analyze Every Transaction in the Fight Against Fraud: Using
Technology for Effective Fraud Detection,” ACL Services Ltd.,
2008.

“The ‘Big Picture’ of Insider IT Sabotage Across U.S. Critical
Infrastructures.” Carnegie Mellon, maio de 2008.

Cappelli, Dawn; Trzeciak, Randal; Moore, Andrew, “Insider Threats
in the SDLC,” CERT, 2006.

Cline, Jay, “530M Records Exposed, and Counting,” Computerworld
Security, 9 de setembro de 2008.

Coderre, David G., Computer Aided Fraud Prevention and
Detection: A Step-by-Step Guide, John Wiley & Sons, 2009.

Coderre, David G., Fraud Analysis Techniques Using ACL, John
Wiley & Sons, 2009.

“Data Breaches Surpass 2007 Level, But Businesses Are Rarely
Penalized,” The Wall Street Journal, 9 de setembro de 2008.

“Fraud Risk Management: Developing a Strategy for Prevention,
Detection, and Response,” KPMG International, 2006.

Global Technology Audit Guide 3: Continuous Auditing:
Implications for Assurance, Monitoring, and Risk Assessment;
The IIA; 2005.

Global Technology Audit Guide 5: Managing and Auditing Privacy
Risks, The IIA, 2006.

“How Fraud Hurts You and Your Government Organization,”
Website da Association of Certified Fraud Examiners: [http://
www.acfe.com/resources/fraud-tools.asp?copy=video](http://www.acfe.com/resources/fraud-tools.asp?copy=video).

“Insider Threat Study: Illicit Cyber Activity in the Information
Technology and Telecommunications Sector,” U.S. Secret Service
e CERT Coordination Center/SEI, janeiro de 2008.

Internal Audit 2012: A Study Examining the Future of Internal
Auditing and the Potential Decline of a Controls-centric
Approach, PricewaterhouseCoopers, 2007.

International Professional Practices Framework. Guia Prático,
Internal Auditing and Fraud. The IIA, 2009.

Lanza, Richard B.; Brooks, Dean; e Goldman, Mort; The Buyer’s
Guide to Audit, Anti-Fraud, and Assurance Software; Ekaros
Publishing, 2008.

Lanza, Richard B. e Gilbet, Scott, “Maximizing Journal Entry
Testing Through Automation,” ITAudit, 10 de fevereiro de 2007.

Lanza, Richard B., “Proactive Control Monitoring,” ITAudit, 15 de
novembro de 2003.

Lanza, Richard B., “Proactively Detecting Fraud Using Computer
Assisted Audit Reports,” The IIA Research Foundation, 2003.

Management Anti-fraud Programs and Controls: Guidance to Help
Prevent, Deter, and Detect Fraud; AICPA, The IIA, Association
of Certified Fraud Examiners (ACFE), Information System
Accountability and Control Auditors, Financial Executives
Institute, Institute of Management Accountants, e Society of
Human Resource Professionals; 2002.

Managing the Business Risk of Fraud: A Practical Guide; The IIA,
ACFE e AICPA; 2008.

“Sample Fraud Policy,” Website da ACFE, [http://www.acfe.com/
documents/sample_fraud_policy.pdf](http://www.acfe.com/documents/sample_fraud_policy.pdf).

SOX Section 404: A Guide for Management by Internal Controls
Practitioners, Segunda Edição, The IIA, 2008.

Site do U.S. Department of Justice, Seção de Computer Crime and
Intellectual Property, <http://usdoj.gov/criminal/cybercrime>,
2009.

Sobre os Autores

- **Ken Askelson**
CIA, CPA, CITP, aposentado pela JC Penney Co. Inc.
- **Rich Lanza**
CPA, CFE, PMP, Presidente da Cash Recovery Partners, LLC
- **Peter Millar**
Diretor de *Technology Application*, ACL Services Ltd
- **Marilyn Prosch**
Ph.D. pela *W.P Carey School of Business*, Professora Associada do *Department of Information Systems Management* da Arizona State University
- **Donald E Sparks**
CIA, CISA, ARM, Vice-Presidente, Audimation Services, Inc.

Revisores e Contribuintes

O The IIA agradece as seguintes organizações e indivíduos que fizeram comentários valiosos e agregaram imenso valor a este guia:

- *Association of Certified Fraud Examiners*
- *Professional Practices Advisory Council*:
 - *Advanced Technology Committee*
 - *Board of Regents*
 - *Committee on Quality*
 - *Ethics Committee*
 - *Internal Auditing Standards Board*
 - *Professional Issues Committee*
- The Institute of Internal Auditors – Reino Unido e Irlanda
- Douglas J. Anderson, The Dow Chemical Company, EUA
- David Bentley, consultor independente, Reino Unido
- Denny K. Beran, JC Penney Co. Inc., EUA
- Lily Bi, The Institute of Internal Auditors, EUA
- David Coderre, *Office of the Comptroller General of Canada*
- John D. Gill, *Association of Certified Fraud Examiners*
- Larry Harrington, Raytheon Company, EUA
- Steve Hunt, Crowe Horwath LLP, EUA
- David Lione, consultor independente, EUA
- Susan Lione, The Institute of Internal Auditors, EUA
- Jay R. Taylor, General Motors, EUA
- Karine Węgrzynowicz, Lafarge SA, França

Sobre o IPPF

O *International Professional Practices Framework* (IPPF) é o *framework* conceitual que organiza as orientações fidedignas promulgadas pelo The Institute of Internal Auditors. As orientações do IPPF incluem:

Orientações Obrigatórias

A conformidade com os princípios estabelecidos nas orientações obrigatórias é necessária e essencial para a prática profissional da auditoria interna. As orientações obrigatórias são desenvolvidas seguindo um processo de *due diligence* estabelecido, que inclui um período de exposição pública para a contribuição dos stakeholders. Os três elementos obrigatórios do IPPF são a Definição de Auditoria Interna, o Código de Ética e as *Normas Internacionais para a Prática Profissional de Auditoria Interna* (*Normas*).

Elemento	Definição
Definição	A Definição de Auditoria Interna indica o propósito fundamental, a natureza e o escopo da auditoria interna.
Código de Ética	O Código de Ética estabelece os princípios e expectativas que regem o comportamento dos indivíduos e organizações na condução da auditoria interna. Ele descreve os requisitos mínimos para conduta e as expectativas comportamentais, em vez de atividades específicas.
Normas Internacionais	As <i>Normas</i> são focadas em princípios e fornecem um <i>framework</i> para realizar e promover a auditoria interna. As <i>Normas</i> são requisitos obrigatórios que consistem em: • Declarações dos requisitos básicos para a prática profissional de auditoria interna e para a avaliação da eficácia de seu desempenho. Os requisitos são aplicáveis internacionalmente, nos níveis organizacional e individual. • Interpretações, que esclarecem os termos ou conceitos dentro das declarações. É necessário considerar as declarações e suas interpretações para entender e aplicar as <i>Normas</i> corretamente. As <i>Normas</i> empregam termos que receberam significados específicos incluídos no Glossário.

Orientações Fortemente Recomendadas

As orientações fortemente recomendadas são apoiadas pelo The IIA por meio de um processo formal de aprovação. Elas descrevem práticas para a implementação eficaz da Definição de Auditoria Interna, o Código de Ética e as *Normas* do The IIA. Os três elementos fortemente recomendados do IPPF são as Declarações de Posicionamento, as Práticas Recomendadas e os Guias Práticos.

Elemento	Definição
Declarações de Posicionamento	As Declarações de Posicionamento auxiliam uma ampla gama de stakeholders, incluindo aqueles que não pertencem à profissão de auditoria interna, a entender questões significantes de governança, riscos ou controle e a delinear as funções e responsabilidades relacionadas à auditoria interna.
Práticas Recomendadas	As Práticas Recomendadas auxiliam os auditores internos na aplicação da Definição de Auditoria Interna, do Código de Ética e das <i>Normas</i> e na promoção de boas práticas. As Práticas Recomendadas tratam da abordagem, metodologias e consideração da auditoria interna, mas não detalham processos ou procedimentos. Elas incluem práticas relacionadas a: questões internacionais, nacionais ou específicas do setor; tipos específicos de trabalhos; e questões jurídicas ou regulatórias.
Guias Práticos	Os Guias Práticos fornecem orientação detalhada para a condução das atividades de auditoria interna. Eles incluem processos e procedimentos detalhados, como ferramentas e técnicas, programas e abordagens passo a passo, além de exemplos de entregáveis.

Este GTAG é um Guia Prático do IPPF.

Para outros materiais fidedignos de orientação, por favor, visite www.theiia.org/guidance-standards.

Prevenção e Detecção de Fraudes em um Mundo Automatizado

À medida que a tecnologia avança, o mesmo acontece com esquemas para cometer fraudes. A tecnologia não pode ser usada apenas para perpetrar fraudes, mas também para preveni-las e detectá-las. O uso da tecnologia para implementar programas de prevenção e detecção de fraudes em tempo real permitirá que as organizações reduzam o custo da fraude, diminuindo o tempo entre o momento em que a fraude é cometida até o momento de sua detecção.

Por meio de um processo passo a passo para auditar programas de prevenção de fraudes, uma explicação dos vários tipos de análise de dados para detectar fraudes e um modelo de avaliação de riscos de fraudes tecnológicas, o GTAG pretende informar e orientar os *chief audit executives* e auditores internos sobre como usar a tecnologia para ajudar a prevenir, detectar e responder a fraudes.

Gostáramos do seu feedback! Visite a página do GTAG em www.theiia.org/gtags para avaliá-lo e enviar seus comentários.



**The Institute of
Internal Auditors**

www.theiia.org

Order Number: 1069
ISBN: 978-0-89413-680-1

IIA Member Free
Nonmember US \$25