GLOBAL PERSPECTIVES & INSIGHTS

FRAUD

PART I: Fraud in the Cryptosphere

PART 2: Internal Auditors and Fraud Examiners: A Valuable Partnership

PART 3: The Hangover: Fraud in the Post-COVID Era

The Institute of Internal Auditors

Contents

Part 1

Fraud in the Cryptosphere

About the Experts

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

Dana Lawrence is Fideseo's Chief Compliance Officer. She is a recognized expert and leader in complex compliance, enterprise risk management (ERM), internal audit, and governance program creation, scaling, and remediation. Lawrence's career in technology and financial services spans mortgage, community banking, large U.S. and global banks, open banking partners, fintech, and crypto. She's held senior leadership roles, working directly with banking regulators and internal/external auditors. Lawrence is a popular public speaker and event host, speaking at local, national, and global events with up to 40,000 participants. She is a committed volunteer and thought leader, serving various groups such as The IIA.

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

Lourdes Miranda is the Chief Compliance Officer for SendCrypto, a blockchain technology company. She is a former CIA Officer and FBI Analyst with 20+ years of government and corporate experience, specializing in financial crime investigations and intelligence collection and analysis globally. She has extensive field experience targeting money launderers and terrorist financiers. Since 2017, Miranda has been working for FinTechs as a senior crypto investigator, senior compliance officer, and risk manager, building compliance, investigation, crypto, and intelligence teams and training programs. She is also an author, instructor, and contributor to multiple online courses as a subject matter expert. Additionally, Miranda is an Advisory Board Member for Canada-based Toronto Compliance & AML Enterprise (TCAE).

Introduction

Crypto and fraud in global conversation

Sam Bankman-Fried, the charismatic founder of cryptocurrency exchange FTX, was once worth an estimated $26.5 billion. As the leader of what was at one point the third-largest exchange in the crypto market, Bankman-Fried and FTX were the darlings of a variety of high-profile investors such as BlackRock and NFL player Tom Brady. Yet, he lost all of his wealth virtually overnight in one of the most dramatic company collapses in modern history.

Bankman-Fried was arrested on December 13, 2022, in the Bahamas. According to published reports, he faces various charges including wire fraud, wire fraud conspiracy, securities fraud, securities fraud conspiracy, and money laundering.

While there is a human interest in the sheer spectacle of such an incredible downfall, the event has also raised greater questions regarding digital assets. With parallels to scandals such as Tornado Cash and Bitzlato, FTX's collapse and the subsequent impact on the industry it represented has led many to question the long-term viability of crypto assets — at least in its current state, which U.S. Securities and Exchange Commission Chairperson Gary Gensler called the "Wild West."

Despite being built on blockchain technology, which is among the most secure ways to maintain crypto assets and information, if the very visible head of one of the world's most prominent cryptocurrency exchanges can allegedly commit acts of large-scale fraud, what other vulnerabilities might exist for companies that operate in the industry in some capacity? How has the risk landscape changed with the meteoric rise of crypto assets, and how are some organizations and their internal audit functions successfully responding to these changes?

Part 1 of this three-part series on fraud will address these questions by examining the common fraud schemes seen in the early stages of a crypto-asset world. For more information on this topic, The IIA will be hosting a replay of its recent webinar "Fraud perspectives: Blockchain, Crypto, and KYC", along with a live Q&A with the subject matter experts cited in this brief.

Uncertainty in the Cryptosphere

An exciting, but risky, future

Organizations are now paying attention

Although its implications are vast and nothing short of revolutionary, blockchain technology is relatively easy to understand conceptually as nothing more than a continuous, ever-growing log of digital asset transactions that can be shared and stored in virtually any network structure. What sets it apart is that it uses verification methodologies that continuously encrypt the block with every new transaction, making it more secure.

“The technology itself is extremely complicated and takes years of training and education to analyze, but I think of the blockchain itself as a financial statement,” said Lourdes Miranda, chief compliance officer for SendCrypto, a blockchain technology company. “The blockchain has information relating to who sent the assets, where they were deposited, if there were any withdrawals, and the resulting balance.”

Cryptocurrency is arguably the most well-known asset that utilizes this technology, which creates a decentralized, open-source monetary system (or systems) immune from the influence of entities, such as central banks — but other examples of crypto assets based on blockchain include non-fungible tokens (NFTs), distributed ledger technologies (DLTs), game tokens, among others.

However, as industries are quickly learning, just because crypto assets are built on secure technology virtually impossible to manipulate by traditional methods does not mean that its adopters are immune from risk. The FTX collapse illustrates this in more ways than one. For example, it illustrated just how damaging the lack of proper corporate governance and internal controls can be, not just for the organization, but for investors throughout the entire industry landscape.

This was a point IIA President and CEO Anthony Pugliese made in a recent letter to the U.S. Congress that called for them to establish new requirements to bolster corporate governance at cryptocurrency exchanges, blockchain technology companies, NFT marketplaces, and Web3 platforms operating in the United States. “Countless investors are now paying the price for FTX’s failures,” said Pugliese. “It’s clear that we cannot rely on unregulated crypto exchanges to do the right thing on their own — we need to mandate stronger corporate governance standards and ensure accountability when these exchanges aren’t protecting their customers. When bad corporate actors fail, it shouldn’t be investors who are left holding the bag.”

Pugliese emphasized FTX’s collapse, and its market consequences could have been mitigated through the actions of a sound internal audit function. “The FTX collapse is the latest reminder that organizations without a robust internal audit function are, at best, playing with fire and, at worst, setting themselves and their stakeholders up for a disastrous – and entirely preventable – fall,” he said.

These concerns from Pugliese and others did not fall on deaf ears. On January 3, 2023, the Federal Reserve, Federal Deposit Insurance Corp (FDIC) and the Office of the Comptroller of the Currency (OCC) released their first-ever joint statement on cryptocurrency. In it, they highlighted a variety of risks that could be in play for banking organizations operating in cryptocurrency in some form, including:

- Risk of fraud and scams among crypto-asset sector participants.
- Legal uncertainties related to custody practices, redemptions, and ownership rights.
- Inaccurate or misleading representations and disclosures by crypto-asset companies.

- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.
- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.
- Heightened risks associated with open, public, and/or decentralized networks, or similar systems.

While all of these risks are worthy of discussion (and in many cases applicable to organizations beyond banks dabbling in crypto), this brief will limit the focus to acts of fraud committed on crypto participants and the prominent forms they take in the current environment.

A Landscape Ripe for Fraud

An ever-expanding risk landscape

A new tool in the bad actor's toolbox

While crypto assets have a litany of advantageous characteristics such as transparency and remarkably advanced encryption against manipulation, these same characteristics have made these assets (and the blockchain technology behind it) a powerful tool for those looking to commit fraud.

Indeed, it is this appeal to bad actors that has drawn the attention of regulators and law enforcement. "The only reason why regulars care about crypto assets is because bad actors are using it to finance operations and launder money," said Miranda, who researched financial crimes for the CIA and FBI for nearly 30 years. "Blockchain is very difficult to manipulate, but it can be utilized in ways that promote nefarious activity."

One method, for example, is the use of false identification identities within the blockchain. "This is huge in the cryptosphere," said Miranda. "Bad actors will use legitimate, valid identities purchased on the black market to pass the KYC [Know Your Customer] onboarding process when they open wallets. These identities do not have a criminal background and are not on any blacklist — they are completely clean. Then, under this clean name, they can move money around largely undetected until investigators can view tell-tale fraud trends with their own eyes."

The crypto asset industry has also introduced a variety of tools that, while designed for consumer convenience, have a variety of loopholes that can be exploited. A fraud initiator, for example, can make use of a crypto transaction hub such as a Bitcoin ATM, along with a burner phone to avoid pings from law enforcement.

"Let's say I'm in New York, and I want to move money in finance, and I have to pay my bad actors in Miami. They want to be paid and paid fast. I'm not going to get a check, and I can't use a computer or laptop, because the IP address pings, so what I do is go to a Bitcoin ATM in New York and use cash and a burner phone. This way, I can pay people while circumventing anti-money laundering protocols. That's fraud," said Miranda.

Pig butchering

Another common fraud tactic that bad actors can utilize is known by the graphic term "pig butchering." "This is basically the concept of a fraudster metaphorically 'fattening up' their victim by investing a lot of time with them in order to establish trust," said Dana Lawrence, chief compliance officer at business and technology consultant firm Fideseo. The time invested by fraudsters can happen anywhere, according to Lawrence, but it most prominently is done either on social media or through texts over the course of weeks or months. Lawrence cited LinkedIn specifically as a favored platform, as well as social sites such as Twitter.

In these cases, the bad actor typically will present themselves as an influencer or insider that has successfully invested in cryptocurrency. Over time, they will tout the benefits of cryptocurrency in an effort to get the victim to transfer their assets to them. In some cases, fraudsters have even provided the victim with forged financial statements to make it appear substantial returns are being made.

While it is easy to read these signs and find them fairly obvious to spot, fraudsters in this case have become highly sophisticated. Scamming teams based in countries such as Cambodia and China, for example, have had in-depth training by psychologists in how to make people most vulnerable to making unsound decisions.

“They’ve been trained by psychologists to try to figure out the best way to manipulate people,” said Santa Clara County, California, district attorney Jeff Rosen in an interview with CNN. “You’re dealing with people that are going to use different psychological techniques to make you vulnerable and to get you interested in parting with your money.”[1]

Pump and dump

The other major fraud form being seen in the cryptosphere is well-known to long-time observers of the stock market: the so-called “pump and dump” scheme.

“This scheme typically starts with a group coming together to start a new crypto project such as a token, and then uses — commonly with the help of influencers — resources to hype it up on platforms such as Twitter or Discord,” said Lawrence. “There’s currently a lot of fluctuation in the crypto market due to liquidity. So, if a lot of people try to buy something all at once, it kind-of shocks the market into raising the price. If this happens, the bad actors in question holding large amounts of the asset suddenly sell it off for a profit, dropping the price suddenly and leaving all other investors with something worth essentially zero.”

The red flag in these situations, said Lawrence, is a distinct lack of disclosures that indicate to potential investors that losing everything is a distinct possibility. The actors will also typically make strong use of copy-and-pasted messages on social media and discussion boards written by posters with similar screen names. And, once the scheme is complete, these screen names will usually disappear, their anonymity completely intact.

Other fraud examples in a crypto asset context

Crypto-based fraud does not always have to be so sophisticated. Within crypto-based organizations, often all that is necessary for a bad actor is the right opportunity. For example, while the blockchain itself will keep digital assets secure, all that is needed to bypass security and empty a crypto wallet is obtaining a private key — a long stream of numbers that could fit on a restaurant napkin and be left anywhere for anyone one to find.

"Your private key is your digital identity to the cryptocurrency market, and anyone who gets hold of this can perform fraudulent transactions or steal your crypto coins,” said Lawrence. “If someone somehow gains access to that, and they took all my Bitcoin out, there's nothing I can do about it. I can't get it back, I can't file a complaint, there's no consumer protection agency or regulator to dispute it with — it's literally gone."

As the crypto market matures, crypto security services have emerged that specialize in protecting individual and company keys from misplacement, but in some cases their methodologies are surprisingly primitive. According to Lawrence, the solution some of these services employ is storing the keys in vaults on the side of desolate mountains. Crypto insurance also exists as a safety net for companies who can afford it, but at this stage the entire industry is struggling with profitability, forcing insurers to be incredibly selective while simultaneously offering coverage that has been shrinking by the year.

In an article published in the U.K.’s Insurance Times, RPC Insurance group partner James Wickes discussed the challenges of the crypto insurance market. “The relatively small number of insurers currently active in the crypto asset insurance space are likely to be keen to review the fine print on policy wordings to limit potential exposure from the volatility of the crypto markets, as demonstrated by the recent crash,” he said. “The insurance market for these assets is in its infancy and it remains to be seen whether a sufficient body of insurance carriers will be prepared to provide enough capacity to meet the demand and how brave the market will be to extend coverage beyond the traditional theft risk.”[2]

Despite these precautions, however, there remain certain tools bad actors can use to still utilize crypto assets and blockchain without directly bypassing an established account — namely mixers, also known as tumblers. One of the core features of a blockchain is its transparency; within any blockchain explorer, anyone can view the record of all blockchain

1. Josh Campbell, “Beware the ‘Pig Butchering’ Crypto Scam Sweeping Across America,” December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.
2. Isobel Rafferty, “Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments,” Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

transactions since the launch of cryptocurrency in 2009. Mixers allow the user to essentially jumble the amount of crypto assets in question before delivering them to intended recipients, giving them a degree of anonymity since it is so difficult to decipher exactly who sent how many assets to whom. Using a mixer, all an explorer will show is that one person, as well as dozens of other people, sent assets to a mixer, and then sent the assets in varied amounts to a variety of other people. The result, in essence, resembles a perfected form of money laundering.

Facing these realities, organizations that choose to exist in the crypto sphere must accept that they are largely on their own when it comes to risk mitigation at this stage. This does not mean that crypto should be avoided, but it does mean that compliance, sound internal control, fraud detection and deterrence efforts, and internal audit must play an outsized part in crypto conversations from the board level down.

Where Internal Audit Can Start

Regulation is here with more to come

Issued guidance resources

As previously mentioned, the regulatory frameworks companies can look to for handling security and governance regarding crypto assets and associated fraud-based risks is scant. However, certain industries such as financial services are not entirely bereft of resources that address proper governance principles regarding digital asset protection — many of which are applicable to cryptocurrency.

In October 2022, the European Union introduced the agreed-on text of The Markets in Crypto-Assets (MiCA) Regulation, which is one of the first attempts globally at comprehensive regulation of cryptocurrency marketing, although the legislation has been tabled until April 2023 to translate it into 24 different languages. Should it be formally adopted, the regulation will:

- Officially define crypto asset as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology." Additionally, it offers four different categories of crypto-asset: asset-referenced tokens, e-money tokens, utility tokens, and a fourth category for crypto-assets that do not fall in the other three categories.
- Officially make crypto providers liable if they lose investors' crypto assets.
- Requires actors in crypto-asset markets to declare information on their environmental and climate footprint.
- Overlap with updated legislation on anti-money laundering, and will task the European Banking Authority (EBA) with maintaining a public register of non-compliant crypto-asset service providers.
- Require crypto-asset providers to have authorization to operate in the EU.
- Provide a strong framework applicable to "stablecoins" (cryptocurrency that is pegged to an external reference asset), which will require every stablecoin holder to be offered a claim at any time by the issuer, free of charge.[3]

In the U.S., a joint statement from the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) offers a few resources for U.S. firms that provide guidance designed to help "banking organizations engage in robust supervisory discussions regarding proposed and existing crypto-asset-related activities."[4] These include:

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

3. General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.
4. "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

These are hardly the only resources available. In the wake of the FTX collapse, the SEC also released guidance that advised companies to disclose their involvement with digital commodities firms.

The value of education

Assuming it is adopted, the proposed EU legislation would take effect in 2024, but it almost certainly will not be the last. As the patchwork regulatory landscape fills in month to month, the most valuable action an internal auditor can take is to make every effort to stay abreast of the changes and clearly articulate those changes to the board and applicable stakeholders.

In the current environment, internal auditors should also articulate to stakeholders what other regulations do exist that may be applicable to their crypto efforts. For example, said Lawrence, a company offering their own cryptocurrency may require registration with the U.S. Financial Crimes Enforcement Network — a critical detail that could be easily overlooked because crypto is not specifically cited in the legislation. “There is a lot of uncertainty now,” she said. “It is up to internal auditors to inform leaders about what is applicable and what is not.”

Focus on new technologies should also not distract companies from basic best practices regarding digital asset protection, including the use of a virtual private network (VPN) and proper security, collection, and, when needed, disposal of user profile information — especially consumers. “User profiles are a critical organizational control,” said Miranda. “If I was auditing a company, I would check to make sure user profiles match transactional activity. For example, geographical information is incredibly important in compliance and investigations. Organizations need to keep this information secure, as well as know where it resides.” On this point, Miranda noted that organizations often overlook non-disclosure agreements (NDAs), which contain critical profile information such as physical addresses that can be critical to a fraud investigation.

For more information, The IIA’s Supplemental Guidance “Internal Audit and Fraud: Assessing Fraud Risk Governance” offers clear direction regarding organizational roles and responsibilities for sound fraud risk governance and management, as well as recommendations for additional guidance such as COSO’s Fraud Risk Management Guide.

Conclusion

Internal audit is ready

Cryptocurrency and the technology that it is based on are too revolutionary for internal audit to ignore, with stakes that more than deserve the attention of the board. Risk assessments that ignore it have a critical blind spot. Cryptocurrency may be a relatively new concept for many, but it does not diminish the value of a sound fraud risk management framework that can be measured and tested by internal audit.

While it is easy to bemoan yet another risk area to add to internal audit's ever-growing radar, the good news is that no other organizational department is positioned better to address it. Much like the Sarbanes-Oxley Act (SOX) did in 2002, the evolution of cryptocurrency regulation virtually assures internal audit a valued position at the table for years to come. Even if the function does not yet know crypto, it does know fraud, and it does know risk; that alone is enough to prime internal audit to take a position of leadership tackling the challenges ahead.

Part 2

Internal Auditors and Fraud Examiners: A Valuable Partnership

About the Experts

Mason Wilder, CFE

Mason Wilder is a Certified Fraud Examiner, and research manager for the ACFE. In this role, he oversees creation and updates of ACFE materials for continuing professional education, assists with the planning and production of all ACFE training events, works on research initiatives such as the Report to the Nations and benchmarking reports, conducts trainings, writes for ACFE publications, and responds to member and media requests. Prior to joining the ACFE, Wilder worked in corporate security intelligence and investigations for over a decade, specializing in background and due diligence investigations and intelligence analysis for international physical security and crisis response. Mason has built a career on gathering relevant information from all sources to analyze and distill in support of critical decision making and is passionate about helping anti-fraud professionals continuously improve their abilities to effectively fight fraud.

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

Shawna Flanders, director of product development at The Institute of Internal Auditors (IIA), is a passionate technologist and technical training industry professional with a passion to adapt technical conversations into common business language. Shawna brings a unique complimentary combination of skills to every engagement, including: SME Content Development/Contribution, Speaking/Training, IT Related Risk, IT Audit, Information and Cybersecurity, IT Compliance, IT Governance, Vendor Management, IT Generalist in Telecom, Programming, Voice and Data Related Architecture Design/Review, Engineering, Analytics and Integration Management, Business Process Management, Business Analysis, Project Management, Program Management and Process Improvement/Six Sigma.

Introduction

Internal auditors provide constructive insights on governance, risks, and internal controls that help organizations manage risks, including identifying and mitigating fraud. However, while internal audit is an effective part of fraud detection and deterrence, finding fraud is not the job of the internal auditor. A Certified Fraud Examiner (CFE), on the other hand, is specifically tasked with identifying and investigating fraud. The CFE brings specialized skills to the battle against fraud. As a result, it makes sense for the two types of professionals to collaborate in a partnership that serves the organization's best interests.

This Global Knowledge Brief, the second in a three-part series on fraud, examines the benefits of building a symbiotic relationship between internal auditors and CFEs.

The Scope of Fraud

Average loss nearly $1.8 million

Fraud remains pervasive risk

Fraud is any illegal act that involves deceit, concealment, or violation of trust that is conducted for a financial or personal gain. The people or organizations that commit fraud may be seeking to steal money, property, or services; to avoid paying for or losing something; or to gain a personal or business advantage. In addition to external scammers, frauds also can be perpetrated by company employees who are experiencing financial pressures or who feel that they are owed the money or services they take because they perceive the organization has treated them unfairly or due to some other grievance. Any type of organization may be a victim of fraud, no matter its size or whether it is public or private, a not-for-profit, a government agency or public or private utility, or other entity.

Fraud is a serious and pervasive risk for organizations. The consequences of fraud can range from disruptive to dire. They can include not only financial challenges and losses, but also inefficiencies that damage operations, revenues, or profits; the cancellation of projects; and, depending on their scope, potentially the failure of the organization.[5]

A survey of CFEs throughout the world by the Association of Certified Fraud Examiners (ACFE) covered 2,110 cases of fraud from 133 countries. Within that group, global losses due to fraud totaled more than $3.6 billion, with an average loss per case of nearly $1.8 million. Indeed, CFEs estimate that organizations lose 5% of their revenue to fraud every year. Smaller companies were clearly at the greatest risk for fraud: Those with the fewest workers experienced the highest median loss, of $150,000.

While losses of that size might be easy to spot, fraud often happens in smaller increments over time. A typical fraud scheme can result in a loss of $8,300 a month and can take 12 months to detect, according to the survey. It's also important to be aware that cryptocurrency is involved in some frauds. The ACFE found that they were involved in 8% of cases. The usual scenarios involved making bribery and kickback payments and converting misappropriated assets.[6]

Categories of Occupational Fraud

There are three primary categories of occupational fraud, according to the ACFE 2022 *Report to the Nations*.

Financial statement fraud schemes or causing a material misstatement or omission in the organization's financial statements, were the least common (9%) but the most expensive, at $593,000 in losses per case.

Asset misappropriation, in which an employee steals or misuses company resources, occurred in 86% of cases. However, it was responsible for the lowest median losses: $100,000 per case.

Corruption, which covers bribery, conflicts of interest, and extortion, was involved in 50% of cases and led to losses of $150,000 per case.

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

[5] [5] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[6] *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

The Role of the Internal Auditor

Assurance/advice on fraud prevention

Fraud detection/deterrence an internal audit mainstay

According to The Institute of Internal Auditors (IIA), "internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. Its role includes detecting, preventing, and monitoring fraud risks and addressing those risks in audits and investigations."[7]

Organizations should not expect internal audit's skill set to include fraud investigation. If circumstances require internal audit to take on an investigatory role, internal auditors should exercise due professional care and should not proceed if they don't have the requisite experience and expertise.

While fraud prevention is the role of management, internal audit supports anti-fraud management efforts by providing necessary assurance services over internal controls designed to detect and deter fraud. Often fraud occurs because of poorly designed controls and weak governance undermining the organization's processes. Nearly half of the cases in the ACFE survey were attributed to a lack of internal controls (29%) or override of existing controls (20%). Auditors consider the potential for fraud risk and the adequacy of internal controls in the areas they examine. When antifraud controls are in place, there tend to be lower fraud losses and quicker detection of fraud, according to the survey.

Internal audit's contribution to antifraud efforts should not be underestimated. When the IIA asked chief audit executives (CAE) to cite where internal audit functions had significant involvement, 57% cited fraud and 56% pointed to overall risk assessment .[8] Meanwhile, the ACFE survey found that the median fraud loss was 50% higher ($150,000 vs $100,000) when there was no internal audit department in place.

Indeed, data from the upcoming 2023 North American Pulse of Internal Audit report finds fraud is the most frequently cited consideration built into internal audits. The annual survey of North American chief audit executives asked more than 500 respondents to indicate which areas they include as part of their audits in general. "Answers indicate that auditors often take a holistic approach and consider a broad range of issues, including cybersecurity, third parties, and governance," according to the report, which will debut in March at the 2023 GAM Conference. Overall, 89% of CAEs said they include fraud considerations in each audit generally, which was the most frequently cited risk category with IT considerations coming in second at 80%

Considerations Integrated into Audits

Source: 2023 North American Pulse of Internal Audit report

The IIA's North American Pulse of Internal Audit Survey, Oct. 20 to Dec. 2, 2022. Q25: When you are conducting audit engagements in general, which of the following areas do you usually include in your considerations? (Choose all that apply.) n = 555.

[7] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[8] 2022 Premier Global Research, *Internal Audit: A Global View*, Internal Audit Foundation, 2022.

According to the IIA Position Paper on *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*,[9] internal audit should have the necessary knowledge of fraud to be able to:

- Identify red flags that may indicate fraud has been committed.
- Understand the characteristics of fraud and the techniques used to commit it, as well as types of fraud schemes and scenarios.
- Be able to decide if further action is necessary or whether an investigation should be recommended.
- Evaluate the effectiveness of controls to prevent or detect fraud and identify opportunities for improvement.

[9] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

The Role of the Fraud Examiner

Investigating deception

Skilled fraud investigation critical

The fraud examiner participates in and supports the organization's overall fraud examination programs. They do this in part by conducting fraud investigations that "seek to obtain facts and evidence to help establish what happened, identify the responsible party, and provide recommendations where applicable."[10] One of the issues an examiner considers in launching an investigation is *predication*, which means that the totality of circumstances must make it seem reasonable to well trained professional that fraud has occurred.

The steps undertaken by a fraud examiner in an investigation might include obtaining evidence, reporting on what is found, testifying on those findings as needed, and assisting in fraud detection and prevention. Two common purposes for a fraud examination are an investigation of a potential fraud or fraud allegation and a review of an organization's anti-fraud policies and controls. More specific objectives behind a fraud examination may include:

- Spotting improper conduct that is or might be associated with fraud, as well as determining who is responsible for any improper behavior.
- Determining the actual or potential losses or liabilities from the fraud.
- Demonstrating the organization's commitment to identifying and mitigating fraud.
- Helping facilitate loss recovery.
- Preventing future fraud and related losses or liabilities.
- Addressing consequences beyond financial losses.
- Finding and strengthening weaknesses in internal controls.
- When required in some instances, complying with statutes, regulations, contracts, or common law duties.[11]

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

Comparing approaches

This table offers an overview of some important differences between the roles, approaches, and goals of internal auditors and CFEs.

Characteristics	Internal audit	Fraud examination
Intention	Internal audit procedures may uncover fraud, but they do not guarantee that they will be detected. For example, auditors may find a suspicious transaction or situation in a review and it may ultimately be identified as fraud. However, finding fraud will only be one aspect of a larger examination of controls and procedures within the area under audit.	A fraud examination is directly focused on uncovering fraud and considering antifraud actions or activities.
Occurrence	Audits are typically regularly recurring, although pop-up audits may be used to address a unique situation or questions in one area.	Fraud examinations are typically only conducted with sufficient predication, although they may occur without any specific trigger as part of a risk management or fraud risk assessment program. However, most are conducted in response to tip or allegation. The ACFE survey found that 43% of frauds were detected because of tips, which was nearly three times the number of the next most common method for finding fraud. More than half of all fraud tips came from employees.
Adversarial or not?	Internal audits are non-adversarial in nature. The auditors' goal is to offer insights and information that team leaders and members can use to improve controls or other processes, for example.	Fraud examinations are inherently adversarial. Part of the goal is to fix blame on whoever is perpetrating the fraud.
Standards	Internal auditors follow the *International Standards for the Professional Practice of Internal Auditing*, set by the Institute of Internal Auditors (IIA).	CFEs follow the ACFE *Code of Professional Standards*. CFEs can use an ACFE fraud risk assessment tool in their examinations.

Putting Collaboration to Work

Mutual Respect and Responsibilities

Working the battle against fraud

There are numerous opportunities for beneficial collaboration between auditors and fraud examiners. They may consult with each other on:

- Launching a fraud investigation
- Annual planning of audit and fraud examinations
- Risk evaluations
- Evaluation and assessment of controls and antifraud programs
- Conveying audit findings with fraud implications
- Remediation of control deficiencies.

Many organizations have rules governing protocols when internal audit hands off a fraud finding to an external or internal fraud examination team. The internal audit team notes the fraud finding and then does a joint report with the fraud examiner at the end of the review.

In addition, internal audit may audit an organization's antifraud dept to ensure that its own controls are adequate. An antifraud team may report to the legal or enterprise risk management teams, among other areas, including internal audit. In the event a fraud team reports to internal audit, any audit of that department should be outsourced to ensure objectivity.

Case study illustrates collaboration at work

The following case study demonstrates how the two teams can work together. It's based on a discussion by Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB, director of product development at The IIA, in a recent IIA and ACFE webinar, *Fostering Collaboration: The Auditor and the Fraud Examiner.*

Typically, internal audit discovers a pattern that mimics fraud and alerts fraud examiners. In the case presented by Flanders, an internal audit included a review of auto loans. One of the steps her team took was to evaluate delinquent accounts. In a group of 40 such accounts, five of them stood out. The system was set to flag delinquent loans that should be followed up, but for some reasons these five were not flagged. In addition, they were all set to have very unusual characteristics: an interest rate of 0%, 72-month terms, and no minimum payment.

When Flanders investigated, she found that the user ID associated with the loans belonged to a customer service representative, which didn't make sense. Someone in this role didn't usually approve loans. She then reviewed the log files related to the loans and found that about one hour before each one was submitted and approved, the holder of the user ID was given additional access to the system. That access was removed about an hour after the loans were approved and activated. Given the unusual loan terms, customer service representative involvement, and changes in system access, the audit team knew it was time to turn the case over to the company's fraud department.

Depending on the organization's policies and procedures, steps the fraud department might take in this case when alerted to the suspicious activity include:

- Corroborate the information received from the auditors.
- Examine the entire scope of activities related to these accounts.
- Determine if the creation of these five accounts was a unique action or part of an ongoing potential scheme.
- Identify any co-conspirators.
- Consider whether other branches or offices are involved and the overall scope of the fraud.

The fraud examiners at this point might also consider whether and how the fraud should be stopped. If more evidence or information is needed, it may be decided that the fraud should be allowed to continue at least temporarily. This is a complicated determination that will depend on how much the company has already lost, how much could be lost potentially if the fraud continues, and the organization's risk appetite, according to Mason Wilder, CFE, research manager at the ACFE, who also participated in the webinar. In this case, steps to take before shutting down the fraud may include interviewing the customer service representative to gain more information and identify the scope of the fraud, and potentially uncover additional frauds or plans for more.

Once they have gathered and analyzed evidence, the fraud examiners would then report their findings—orally or in writing—to the appropriate people in the organization. This might include management, the board, or the audit committee. "A fraud examination report is a narration of the fraud examiner's specific activities, findings, and, if appropriate, recommendations," according to the *ACFE Fraud Examiners Manual*. Organization management can then use the report to determine the appropriate next steps.

If the fraud examiners review the situation and don't find actual fraud, they may hand back the case if they determine that the original red flag arose because of a deficiency in fraud risk management controls. Internal audit could then include this deficiency in its report.

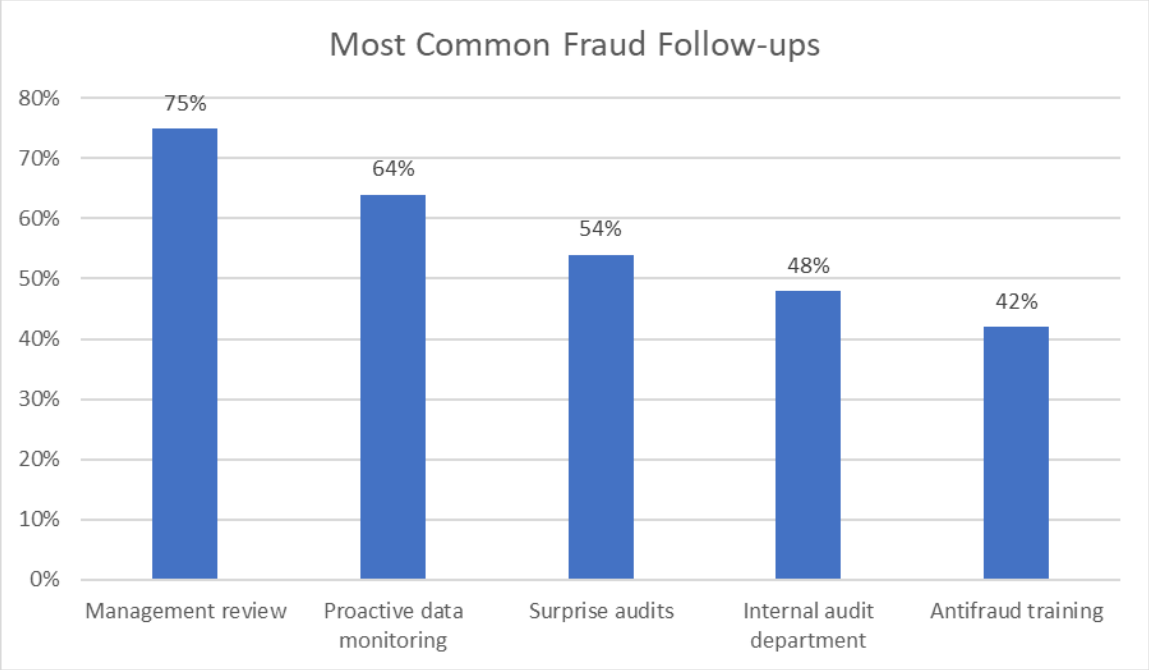
Combining strengths

Those concerned with fraud should remember that mitigation is important. The ACFE survey report noted that proactive steps to find fraud can lead to earlier detection and lower losses, while reactive efforts allow the schemes to play out over a longer time and heighten the financial impact for the victim.

However, organizations cannot identify or eliminate all fraud risks. They face numerous types of fraud, a variety of motivations behind them, and a wide range of perpetrators. However, the more knowledgeable that people are at all levels — management, the board, and staff — the better they will be at deploying reasonable mitigation efforts and identifying fraud or the red flags that may indicate its existence. By combining their unique skills and experience, internal auditors and fraud examiners can make a strong contribution to the organization's overall efforts. Organizations can use their work to make more informed decisions about fraud risk management approaches.

Steps to prevent recurrence

A total of 81% of organizations in the ACFE survey made modifications to their antifraud controls after a fraud. The chart below shows the most typical changes to controls that organizations implemented or modified. Other antifraud controls recommended by the ACFE include automated transaction/data monitoring, surveillance, and account reconciliation.



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

Conclusion

Internal audit's role as the third line provider of assurance over governance, risk, and internal control requires structures, processes, and practices that promote objective and independent assurance. But, as noted in The IIA's Three Lines Model, independence does not imply isolation.

"There must be regular interaction between internal audit and management to ensure the work of internal audit is relevant and aligned with the strategic and operational needs of the organization. Through all of its activities, internal audit builds its knowledge and understanding of the organization, which contributes to the assurance and advice it delivers as a trusted advisor and strategic partner," according to the Model.

This is clearly the case when internal audit and certified fraud examiners find common ground as allies in the battle against fraud.

Part 3

The Hangover: Fraud in the Post-COVID Era

About the Expert

David Dominguez, CIA, CRMA, CPA, CFE

David is director of audit and compliance at Itafos in Houston. In his career, David has worked with multinational companies in various industries to establish, direct, and transform corporate and regional internal audit functions. He has led and executed financial, operational, and IT assurance and advisory projects in North America, Latin America, Europe, and Asia. He also has managed and participated in numerous multi-jurisdictional investigations, data analytics initiatives, and a wide variety of international shareholder, joint venture, and vendor audits. His areas of expertise include corporate and organizational governance, enterprise risk management, fraud risk management, the Sarbanes-Oxley Act of 2002, and ethics and compliance programs.

Introduction

For the better part of two years, COVID-19 caused disruptions across the board, ranging from the way that people worked, where they worked, how their organizations dealt with suppliers and supply chain issues, and how they handled significant concerns, such as maintaining internal controls and detecting and preventing fraud.

Today, the world breathes easier as the worst of the pandemic slowly fades into history, but even still, one should not assume that the risks associated with COVID-19 are no longer a concern. Indeed, organizations that make that assumption could be making a grave mistake. This Global Knowledge Brief, the third in a three-part fraud series from The Institute of Internal Auditors (IIA), examines various pandemic-related fraud factors identified in the *2022 ACFE Report to the Nations*, how they may impact organizations, and internal audit's role in organizational efforts to mitigate those fraud risk factors.

Fraud and Fraud Risks Linger

Pandemic-related changes remain a concern

New COVID-inspired frauds will emerge

In its most recent *Report to the Nations* on occupational fraud, The Association of Certified Fraud Examiners (ACFE) found that the median duration of frauds — that is, the typical time between when a fraud begins and when it is detected — was 12 months.[12] That means that organizations continue to face pandemic-related frauds that have yet to be discovered.

There are many reasons that changes related to the pandemic continue to impact fraud risk. For example, the adoption of remote work was intended to be temporary, but it has turned into standard operating procedure in many companies. Remote work often brought with it significant changes — and in some cases loosening — of practices and procedures designed to identify or mitigate fraud. As a result, associated risks continue to pose threats for companies even as pandemic-related disruptions have waned.

Internal audit has and will continue to play a key role in handling ongoing fraud risks related to the pandemic. In a study of IIA members around the globe done by the Internal Audit Foundation (IAF) and Kroll, many participants in related roundtables felt that the pandemic "put internal audit more in the driving seat when it comes to fraud risk management."[13] This includes added involvement in strategic considerations of operational challenges, providing continuous assurance, and increased collaboration across business functions — all while maintaining auditor independence.

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

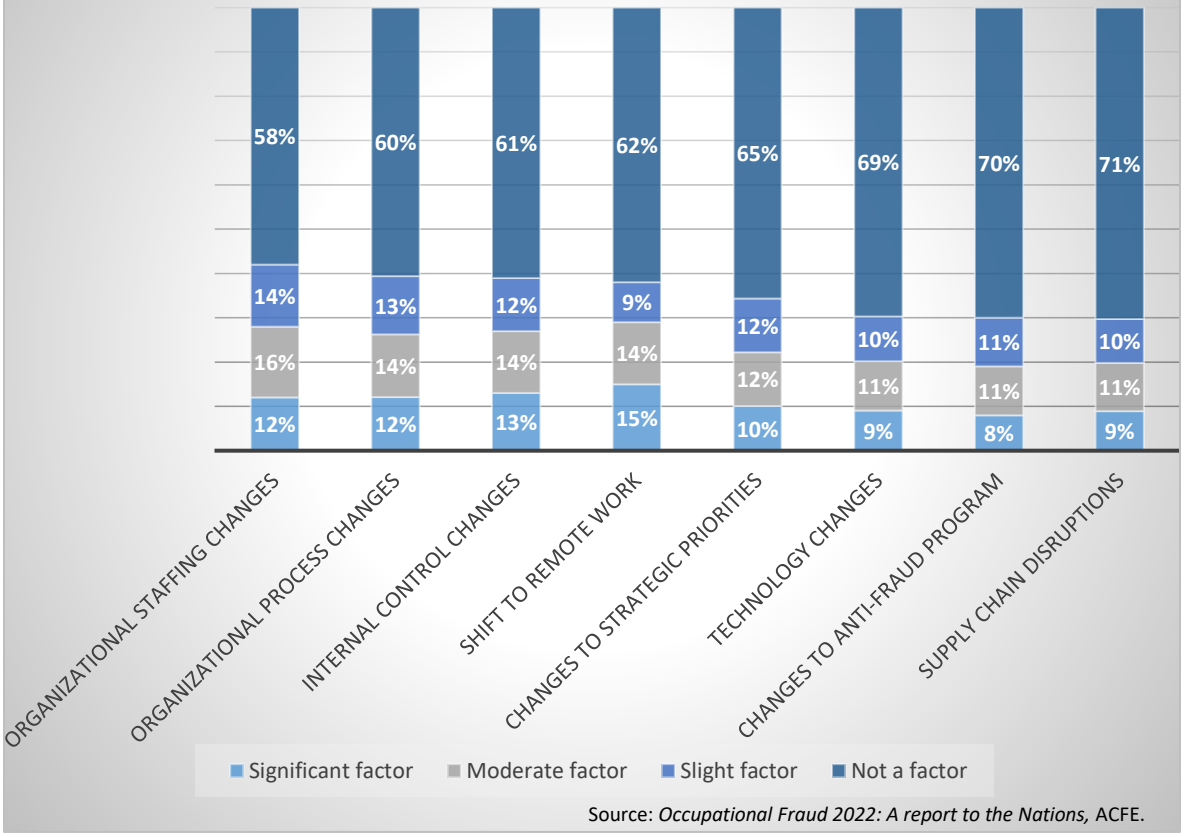
Top Pandemic-Related Fraud Risks

Staffing changes, remote work greatest concerns

More than half see pandemic factors contributing to fraud

In preparing its report on occupational fraud, the ACFE found that 52% of respondents reported that, in fraud incidents they had investigated, at least one of several pandemic-related issues contributed to the fraud. Among them, pandemic-related organizational staffing changes were the most common. A total of 42% of respondents said staffing changes were significant, moderate, or slight factors contributing to occupational fraud. A shift to remote work was the factor most commonly cited as significant (15%), followed by internal controls (13%) (See Figure 1).

Figure 1: How much did pandemic-related factors contribute to occupational frauds?



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

A deeper examination of some of the top pandemic-related issues identified in the ACFE report shows that impacts can often be complex and subtle.

Staffing changes pose various fraud risks

The pandemic forced many organizations to find workarounds or shortcuts in order to navigate the many disruptions they were facing, including changing or expanding workers' responsibilities or bringing in new people who had limited time to acclimate to their jobs. In addition, temporary layoffs or furloughs resulting from pandemic-related economic uncertainty often became permanent, noted David Dominquez, director of audit and compliance at Itafos, a phosphate and specialty fertilizer company. "It definitely increased risk from various angles," he said.

Given the many adjustments and accommodations to work practices and protocols the pandemic may have created — and the potential learning curve for those taking on new tasks — organizations should consider what kinds of unintentional impacts these changes may have had. Here are some areas to consider:

Culture

There are a number of reasons to reassess and perhaps reaffirm corporate culture and values in the wake of the pandemic. "Making it work" was a virtue during the pandemic, but that may mean some important ethical practices and attitudes have been forgotten. New workers may also never have experienced a proper introduction to the company's ethical values. If that is the case, organizations would be well advised to remind employees of their expectations about ethical behaviors.

"A proactive approach to culture can deter various types of misconduct and promote behaviors that can enhance morale and productivity," said the ACFE in its report. "Culture has a powerful ability to affect how people do their jobs; how decisions about quality, compliance, and other critical concerns are made; and how the organization is perceived both internally and externally."[14]

Human resources considerations

A labor shortage and shifting policies on hybrid and remote work have upended some long-standing human resources practices, such as anonymous whistleblower hotlines.

One important HR-related tool in fraud prevention is the anonymous whistleblower hotline. Indeed, 42% of frauds were detected by tips, according to the ACFE report, more than three times as many as the next most common method.

Internal audit can support this process by examining whether it is working as intended. The first step might be determining how well these hotlines are monitored and whether complaints are followed up and tracked, Dominquez said. He recommends asking hotline monitors questions, such as:

- **How do people access the hotline?** Options include leaving tips in a drop box in the office, calling a hotline number, or reporting complaints online. Keep in mind that a drop box — and posters promoting the hotline — will not help remote workers.
- **Can the hotline be made available in different languages, if appropriate?**
- **How well is the effort being tracked?** Dominquez noted that some companies congratulate themselves for low complaint numbers. This could be an accurate reflection of a well-run organization, but it also may indicate that some hotline calls are not answered or complaints are rarely pursued.

Internal audit can review the process for responding to complaints to ensure appropriate timing from intake to resolution and whether decisions to follow up or not are well founded. Organizations sometimes miss valid fraud tips because of fear of retaliation following a complaint. Internal audit can review whether the corporate handbook or code of conduct explicitly prohibits retaliation. Going further, internal audit can also help the company track whether whistleblowers are less likely to get a promotion or more likely to get a poor performance review, Dominquez noted. Even when a complaint is unsubstantiated, companies may find through the response process policies that need updating or clarification, he said.

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

Other valuable precautions/controls organizations should continue or implement include:

- Background checks to identify past credit history or other financial problems or a history of wage garnishments, liens, or judgments that may be associated with embezzlement.
- Verification of credentials.

The ACFE reported that 50% of fraudsters exhibited at least one HR-related red flag before or during the time of the fraud incident. In terms of behavioral clues, living beyond one's means has been the most common red flag in every ACFE study since 2008. It was identified in 39% of cases, well ahead of the second most common factor, financial difficulties, at 25%.

Job uncertainty

The ACFE identified a number of examples of job uncertainty that can contribute to fraud, and challenging economic conditions can heighten such insecurity. The specific red flags include:

- Fear of job loss.
- Denied raise or promotion.
- Cut in benefits.
- Cut in pay.
- Involuntary cut in hours.
- Demotion.

While the economic climate has stabilized since the worst days of the pandemic, challenges remain within the global business climate. Not surprisingly, the impact of issues relating to job uncertainty remained strong in 2022, according to the ACFE. It stands to reason that some of these uncertainties may still be a factor in driving employee misconduct.

These red flags apply to employees generally, but there were a few additional flags that apply specifically to C-suite executives:

- **Bullying or intimidation**. 23% for owner/executives; 8% for non-owner/executives.
- **Control issues.** 18% for owner/executives; 12% for non-owner/executives.
- **"Wheeler-dealer" attitude.** 17% for owner/executives; 9% for non-owner/executives.
- **Excessive pressure from within the organization.** 13% for owner/executives; 6% for non-owner/executives.
- **Past legal problems.** 11% for owner/executives; 3% for non-owner/executives.

COVID-related internal control changes should be revisited

Internal controls are procedures adopted to ensure that actions and decisions throughout an organization are in line with its policies, reporting requirements, and compliance mandates. Antifraud controls can reduce fraud losses and make it easier to detect fraud faster. In the ACFE study, nearly half of fraud losses could be traced to two factors: lack of internal controls (29%) and override of existing controls (20%). Implementing and strengthening internal controls can clearly provide a significant positive benefit for organizations. Internal audit has an important role to play in reporting on internal controls and recommending enhancements to them. Indeed, the ACFE survey found that the median fraud loss was 50% higher ($150,000 vs $100,000) when there was no internal audit department in place.

Internal auditors responding to the IAF/Kroll survey believed that "the internal control framework had been weakened due to the challenges of remote working and, in many cases, a reduction of staff through illness, furlough, and headcount."[15]

New people joining organizations during crisis times may not have received sufficient training or transfer of knowledge, or they may have only learned emergency protocols that did not include long-standing processes and controls, Dominquez said. "Controls were diluted or maybe just fell through the cracks," he said. Along the way, such shortcuts may become — and may remain — standard operating procedure even though they were only meant to be used during a specific time frame or in a particular situation.

This concern has led to positive changes in many organizations. For example, roughly three-quarters of audit committee members responding to a joint survey by Deloitte's Center for Board Effectiveness and the Center for Audit Quality said they have updated their internal controls in the last year because of the remote work environment.[16]

Weaknesses in internal controls can contribute to fraud by creating or promoting an environment where neglect or override of robust anti-fraud measures is easier. For example, during the pandemic, segregation of duties — a common and effective anti-fraud measure — may have been set aside because it was more difficult to accomplish with workers scattered across different locations or because of staffing cutbacks or shortages. This is the type of internal control that a company should review now to ensure that it has been reinstated and is working effectively.

Internal audit can help organizations address these risks by ensuring vital protocols and processes are in place. Using process mapping technology, they can track processes over a recent period — six months or year — and identify variations from proper guidelines or best practices. "You can see deviations from standard procedures or policies and identify which processes need to be updated or enforced," Dominquez said.

Other areas to revisit include internal controls related to procurement, check-writing, bank reconciliations, expense reimbursements, or any area involved with financial considerations.

Remote work remains critical fraud factor

The dramatic pivot to remote work — shutting down offices and allowing workers to perform their jobs at home — was likely the most significant change for most organizations during the pandemic. Consequently, this new approach was the factor most cited as significantly contributing to fraud in the ACFE report. In normal circumstances, a company might spend months considering the strategic impact of such a move, but this was essentially impossible amid the uncertainty and urgency of the early weeks of the pandemic. If nothing else, working alone and out of sight of colleagues and supervisors can simply make it easier to perpetrate a variety of frauds. Those who are making or have made a permanent move to remote or hybrid work should engage in change management planning "to discover the fault lines that can have catastrophic consequences if left unaddressed," according to the ACFE.[17]

Through this process, there are several potential fault lines internal audit could focus on. For example, the difficulties of effectively managing people in a fragmented remote environment and its impact on culture were cited as key areas to address, according to the IAF/ Kroll report.[18] Ethical behavior is often something that is learned and reinforced through interactions with other workers who demonstrate it on the job. Access to more experienced colleagues can help employees understand how to respond in confusing or suspicious circumstances, such as when another worker seems to be acting inappropriately or illegally.

Among the types of fraud specifically associated with remote work are:

[15] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[16] *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, January 25, 2022.
[17] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[18] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

- **Time theft or making inaccurate claims on hours worked.** This can be easier to do when someone isn't under direct supervision.
- **Data theft or misusing or sharing confidential or sensitive information.** This may be done by those who can gain access to an employee's devices or by employees who feel more comfortable misusing data when away from the office.[19]

A related concern is remote employees taking on secondary jobs. For example, an employee may conduct consulting or temporary assignments for another company during the hours they are supposed to be working for their primary employer, Dominquez said. This is certainly theft of time, but misuse of company resources, such as laptops or phones, may also expose the company to cybersecurity issues. The side job may also be a conflict of interest if the employee is doing work for a competitor, especially if they share information that is beneficial to the competition. Internal audit can help address this problem by questioning the type of training employees receive and whether the employee handbook and policies have been updated for new work environments, Dominquez said.

Technology changes create fraud give and take

Technology can enable organizations to implement effective procedures in areas such as internal controls and remote work. Organizations already were making enhancements and investments in technology to address cybersecurity concerns, and the pandemic spurred companies to accelerate and strengthen their systems. Many internal audit functions were included in the technology upgrade. Indeed, 29% of internal auditors have added data analysis as a tool to identify fraud and corruption since the pandemic began.[20]

At the same time, misuse or neglect of technology tools can make it easier for fraud schemes to succeed. As noted, data theft is one of the concerns associated with remote work. Possible solutions to data theft risks, according to the ACFE, include requiring workers to secure their home network — and not share them with other family members. The use of VPNs and stronger and more complex passwords and settings to secure home computers are also key. Other options include multi-factor authentication and annual training for employees on data security and privacy. Organizations should also develop policies on acceptable use of electronic devices, social media, and company data, as well as require employees to read and acknowledge they understand the policies.

Organizations working in a remote or hybrid environment will also need to ensure that employees update software and security patches on their home devices, as well as educate workers about the best ways to avoid phishing and other hacker threats.[21] Of course, companies that scrambled to keep up with the pandemic's impact should review their own cybersecurity measures to ensure they remain up to date.

To help address these concerns, Dominquez recommended that internal audit can investigate what security protocols are in place, what data loss prevention tools the organization is using, if it requires multi-factor authentication and VPNs, and if accounts are timely deactivated when employees leave.

"Quiet Quitting" impacts compliance, ethics efforts

"Quiet quitting" refers to a practice where workers do only the bare minimum of their job requirements. According to one estimate by Gallup, such workers make up at least 50% of the U.S. workforce. The level of engaged workers was at 32%, but those who were actively disengaged was 18%. Gallup notes that this is especially problematic at a time when many jobs are collaborative or when it might take an extra step to meet customer needs. And while the trend toward quiet quitting

[19] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[20] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[21] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.

has gotten a lot of attention, employers should be aware that loud quitters — or people who actively express and perhaps spread their dissatisfaction — still exist.[22]

This trend can be bad news for productivity, efficiency, and retention. At the same time, it can have a negative effect on risk management. "People are not paying as much attention to what they ought to do," Dominquez said. And, as *Corporate Compliance Insights* notes, a successful compliance and ethics program requires the participation and support of everyone in an organization. "When you combine a relatively negative outlook on work with a minimum-viable-work-product approach, the extras that compliance and ethics professionals rely on to make sure people raise issues are often gone," it noted.[23]

That is certainly true of a fraud risk management program, as well. Employees may be rubber-stamping approvals and transactions or ignoring anomalies, or they may escalate an anomaly only to find that their next level-manager has ignored it because they are quiet quitting.

Internal audit can examine employee satisfaction surveys, turnover rates, and exit interviews to get a sense of problems in employee engagement. Recent trends can be compared to activity before the pandemic to understand what impact it may have had, Dominquez said.

[22] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, September 6, 2022.
[23] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, September 14, 2022.

Conclusion

What does all of this add up to? According to ACFE', organizations lose an estimated 5% of revenue to fraud every year, with a median loss of $117,000 and average loss of $1,783,000. Typically, fraud scheme losses can average $8,300 a month. Those are serious considerations for any organization.

During and since the worst of the pandemic, organizations have turned to internal auditors to help strategic decision makers reassess and improve operational processes. This practice should continue, particularly in evaluating anti-fraud internal controls. The world may have emerged from the pandemic, but it has not necessarily shaken off pandemic-related fraud threats.

Since the pandemic began, there has been an even greater appreciation for the contributions that internal audit can make in mitigating or stopping fraud. In the past, internal audit was often brought in after a fraud incident had already occurred. This is changing; organizations are now less likely to wait to detect fraud and hope to address it before too much damage is done. To help accomplish this, they are engaging internal auditors in prevention-based conversations, in other words, asking them to consider anti-fraud controls before fraud happens, Dominquez said. Internal audit is also facilitating discussions on fraud risk assessment and fraud risk assessment frameworks, considering the frequency and effectiveness of those assessments and control testing, and noting any changes in the company's ongoing risk profile. "Instead of waiting to detect fraud, internal auditors are moving to the preventive side," Dominquez said.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 230,000 global members and has awarded more than 185,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

Copyright

April 2023

The Institute of Internal Auditors

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