GLOBAL PERSPECTIVES & INSIGHTS

FRAUD

Teil 1: Fraud in der Kryptosphäre

Teil 2: Interne Revision und Fraudermittler: Eine wertvolle Partnerschaft

Teil 3: Nachwirkungen: Fraud in der Nach-COVID-Zeit

Übersetzung durch

DIIR Deutsches Institut für Interne Revision e.V.

The Institute of Internal Auditors

Inhalt

Teil 1

Fraud in der Kryptosphäre

Über die Experten

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

Dana Lawrence ist Chief Compliance Officer bei Fideseo. Sie ist eine anerkannte Expertin und Führungskraft in den Bereichen komplexe Compliance, Enterprise Risk Management (ERM), Interne Revision sowie Erstellung, Skalierung und Sanierung von Governance-Programmen. Lawrences Karriere in den Bereichen Technologie und Finanzdienstleistungen umfasst Hypotheken, Community Banking, große US-amerikanische und globale Banken, Open-Banking-Partner, Fintech und Krypto. Sie hatte leitende Positionen inne und arbeitete direkt mit Bankenaufsichtsbehörden sowie internen und externen Prüfern zusammen. Lawrence ist eine gefragte Rednerin und Eventmoderatorin und spricht auf lokalen, nationalen und globalen Veranstaltungen mit bis zu 40.000 Teilnehmern. Sie ist engagiert ehrenamtlich tätig, Vordenkerin und unterstützt verschiedene Gruppen wie das IIA.

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

Lourdes Miranda ist Chief Compliance Officer bei SendCrypto, einem Blockchain-Technologieunternehmen. Sie ist ehemalige CIA-Beamtin und FBI-Analystin mit über 20 Jahren Erfahrung in Regierung und Wirtschaft und spezialisiert auf die Untersuchung von Finanzkriminalität sowie die weltweite Sammlung und Analyse von Informationen. Sie verfügt über umfangreiche praktische Erfahrung im Kampf gegen Geldwäsche und Terrorismusfinanzierung. Seit 2017 arbeitet Miranda für FinTechs als leitende Krypto-Ermittlerin, leitender Compliance Officer und Risikomanagerin und baut Compliance-, Ermittlungs-, Krypto- und Geheimdienstteams sowie Schulungsprogramme auf. Sie ist außerdem Autorin, Dozentin und als Fachexpertin an mehreren Online-Kursen beteiligt. Darüber hinaus ist Miranda Mitglied des Beirats des kanadischen Unternehmens Toronto Compliance & AML Enterprise (TCAE).

Einleitung

Krypto und Fraud in der globalen Diskussion

Sam Bankman-Fried, der charismatische Gründer der Kryptowährungsbörse FTX, besaß ein geschätztes Vermögen von 26,5 Milliarden Dollar. Als Leiter der einst drittgrößten Börse im Kryptomarkt waren Bankman-Fried und FTX die Lieblinge zahlreicher namhafter Investoren wie BlackRock und NFL-Star Tom Brady. Dennoch verlor er sein gesamtes Vermögen praktisch über Nacht bei einem der dramatischsten Firmenzusammenbrüche der modernen Geschichte.

Bankman-Fried wurde am 13. Dezember 2022 auf den Bahamas festgenommen. Laut veröffentlichten Berichten werden ihm verschiedene Anklagen vorgeworfen, darunter Überweisungsbetrug, Verschwörung zum Überweisungsbetrug, Wertpapierbetrug, Verschwörung zum Wertpapierbetrug und Geldwäsche.

Zwar ist das Spektakel eines solch unglaublichen Niedergangs für Menschen von Interesse, doch wirft das Ereignis auch größere Fragen in Bezug auf digitale Vermögenswerte auf. Mit Parallelen zu Skandalen wie Tornado Cash und Bitzlato haben der Zusammenbruch von FTX und dessen Auswirkungen auf die gesamte Branche dazu geführt, dass viele die langfristige Rentabilität von Krypto-Assets in Frage stellen – zumindest in ihrem aktuellen Zustand, den der Vorsitzende der US-Börsenaufsichtsbehörde (SEC), Gary Gensler, als „Wilden Westen“ bezeichnete.

Wenn die Blockchain-Technologie zu den sichersten Methoden zur Verwaltung von Krypto-Assets und -Informationen zählt, stellt sich die Frage, ob der prominente Chef einer der weltweit bekanntesten Kryptowährungsbörsen angeblich groß angelegten Fraud begehen kann. Welche weiteren Schwachstellen könnten dann für Unternehmen bestehen, die in der Branche tätig sind? Wie hat sich die Risikolandschaft mit dem rasanten Aufstieg von Krypto-Assets verändert, und wie reagieren einige Unternehmen und ihre Internen Revisionen erfolgreich auf diese Veränderungen?

Teil 1 dieser dreiteiligen Serie zum Thema Fraud befasst sich mit diesen Fragen und untersucht die gängigen Fraudmethoden in der Frühphase der Krypto-Asset-Welt. Für weitere Informationen zu diesem Thema bietet das IIA eine Aufzeichnung seines Webinars „Fraud perspectives: Blockchain, Crypto, and KYC“, sowie eine Live-Fragerunde mit den in dieser Zusammenfassung genannten Fachexperten.

Unsicherheit in der Kryptosphäre

Eine aufregende, aber riskante Zukunft

Organisationen sind jetzt aufmerksam

Obwohl die Auswirkungen enorm und revolutionär sind, ist die Blockchain-Technologie konzeptionell relativ einfach zu verstehen. Sie ist nichts anderes als ein kontinuierliches, ständig wachsendes Protokoll digitaler Asset-Transaktionen, das in praktisch jeder Netzwerkstruktur geteilt und gespeichert werden kann. Das Besondere daran ist, dass sie Verifizierungsmethoden verwendet, die den Block bei jeder neuen Transaktion kontinuierlich verschlüsseln und so für mehr Sicherheit sorgen.

„Die Technologie selbst ist extrem kompliziert und erfordert jahrelange Schulung und Ausbildung, um sie zu analysieren. Ich betrachte die Blockchain jedoch wie eine Art von Finanzberichterstattung“, sagte Lourdes Miranda, Chief Compliance Officer von SendCrypto, einem Blockchain-Technologieunternehmen. „Die Blockchain enthält Informationen darüber, wer die Vermögenswerte gesendet hat, wo sie hinterlegt wurden, ob es Abhebungen gab und wie hoch der daraus resultierende Kontostand ist.“

Kryptowährungen sind wohl die bekanntesten Vermögenswerte, die diese Technologie nutzen. Sie schaffen ein dezentrales, open-source Währungssystem (oder mehrere), das immun gegen den Einfluss von Einrichtungen wie Zentralbanken ist. Weitere Beispiele für Krypto-Vermögenswerte auf Blockchain-Basis sind unter anderem Non-Fungible Tokens (NFTs), Distributed-Ledger-Technologien (DLTs) und Game-Tokens.

Jedoch hat die Industrie schnell gelernt: Nur weil Krypto-Assets auf einer sicheren Technologie basieren, die mit herkömmlichen Methoden praktisch nicht manipuliert werden kann, heißt das nicht, dass ihre Anwender immun gegen Risiken sind. Der Zusammenbruch von FTX verdeutlicht dies in mehrfacher Hinsicht. Er verdeutlicht beispielsweise, wie schädlich der Mangel an geeigneter Governance und internen Kontrollen sein kann – nicht nur für das Unternehmen, sondern für Investoren in der gesamten Branche.

Dies betonte IIA-Präsident und CEO Anthony Pugliese kürzlich in einem Brief an den US-Kongress. Darin forderte er die Einführung neuer Anforderungen zur Stärkung der Corporate Governance bei Kryptowährungsbörsen, Blockchain-Technologieunternehmen, NFT-Marktplätzen und Web3-Plattformen in den USA. „Unzählige Investoren zahlen jetzt den Preis für das Versagen von FTX“, sagte Pugliese. „Es ist klar, dass wir uns nicht darauf verlassen können, dass unregulierte Kryptobörsen von sich aus das Richtige tun – wir müssen strengere Corporate-Governance-Standards einführen und Verantwortlichkeit sicherstellen, wenn diese Börsen ihre Kunden nicht schützen. Wenn schlechte Unternehmen scheitern, sollten nicht die Investoren die Zeche zahlen müssen.“

Pugliese betonte, dass der Zusammenbruch von FTX und die damit verbundenen Marktfolgen durch eine solide Interne Revision hätten abgemildert werden können. „Der Zusammenbruch von FTX ist die jüngste Erinnerung daran, dass Unternehmen ohne eine robuste Interne Revision im besten Fall mit dem Feuer spielen und im schlimmsten Fall sich selbst und ihre Stakeholder einem katastrophalen – und völlig vermeidbaren – Absturz aussetzen“, sagte er.

Diese Bedenken von Pugliese und anderen stießen auf offene Ohren. Am 3. Januar 2023 veröffentlichten die Federal Reserve, die Federal Deposit Insurance Corp (FDIC) und das Office of the Comptroller of the Currency (OCC) ihre erste gemeinsame Erklärung zu Kryptowährungen. Darin hoben sie eine Reihe von Risiken hervor, die für Banken, die in irgendeiner Form mit Kryptowährungen arbeiten, bestehen könnten, darunter:

- Risiko von Fraud und Schwindel unter den Teilnehmern des Krypto-Asset-Sektors.
- Rechtliche Unsicherheiten im Zusammenhang mit Verwahrungspraktiken, Rücknahmen und Eigentumsrechten.
- Ungenaue oder irreführende Darstellungen und Offenlegungen von Krypto-Asset-Unternehmen.
- Erhebliche Volatilität auf den Märkten für Krypto-Assets, die sich unter anderem auf die Einlagenströme von Krypto-Asset-Unternehmen auswirken kann.

- Ansteckungsgefahr innerhalb des Krypto-Asset-Sektors aufgrund von Verbindungen zwischen bestimmten Krypto-Asset-Teilnehmern, unter anderem durch undurchsichtige Kredit-, Investitions-, Finanzierungs-, Service- und Betriebsvereinbarungen.
- Mangel an Reife und Robustheit bei den Praktiken des Risikomanagements und der Governance im Krypto-Asset-Sektor.
- Erhöhte Risiken im Zusammenhang mit offenen, öffentlichen und/oder dezentralen Netzwerken oder ähnlichen Systemen.

Obwohl alle diese Risiken einer Diskussion wert sind (und in vielen Fällen auch auf andere Organisationen als Banken zutreffen, die sich mit Kryptowährungen beschäftigen), beschränkt sich dieser Bericht auf Fraudfälle gegenüber Krypto-Teilnehmern und die häufigsten Formen, die diese im aktuellen Umfeld annehmen.

Eine für Fraud prädestinierte Landschaft

Eine ständig wachsende Risikolandschaft

Ein neues Tool im Werkzeugkasten des Bösewichts

Krypto-Assets verfügen zwar über eine ganze Reihe vorteilhafter Eigenschaften wie Transparenz und eine bemerkenswert fortschrittliche Verschlüsselung gegen Manipulation, aber eben diese Eigenschaften haben die Vermögenswerte (und die Blockchain-Technologie dahinter) zu einem mächtigen Tool für diejenigen gemacht, die Fraud begehen wollen.

Tatsächlich ist es diese Anziehungskraft auf Kriminelle, die die Aufmerksamkeit von Regulierungs- und Strafverfolgungsbehörden auf sich gezogen hat. „Der einzige Grund, warum sich Regulatoren für Krypto-Assets interessieren, ist, dass Kriminelle sie zur Finanzierung von Operationen und zur Geldwäsche nutzen“, sagte Miranda, die fast 30 Jahre lang für die CIA und das FBI Finanzkriminalität erforscht hat. „Blockchain ist sehr schwer zu manipulieren, kann aber auf eine Weise eingesetzt werden, die schändliche Aktivitäten fördert.“

Eine Methode ist beispielsweise die Verwendung falscher Identitäten innerhalb der Blockchain. „Das ist in der Kryptosphäre ein großes Thema “, so Miranda. „Böswillige Akteure nutzen legitime, gültige Identitäten, die sie auf dem Schwarzmarkt erworben haben, um den KYC-Onboarding-Prozess (Know Your Customer) zu bestehen, wenn sie Wallets öffnen. Diese Identitäten haben keinen kriminellen Hintergrund und stehen auf keiner schwarzen Liste – sie sind absolut sauber. Unter dem sauberen Namen können sie dann weitgehend unentdeckt Geld bewegen, bis Ermittler verräterische Fraudtrends mit eigenen Augen erkennen.“

Die Krypto-Branche hat zudem eine Reihe von Tools eingeführt, die zwar auf Verbraucherfreundlichkeit ausgelegt sind, aber auch Schlupflöcher bergen, die ausgenutzt werden können. Ein Betrüger kann beispielsweise einen Krypto-Transaktionsknotenpunkt wie einen Bitcoin-Geldautomaten zusammen mit einem Wegwerfhandy nutzen, um Pings von Strafverfolgungsbehörden zu vermeiden.

„Nehmen wir an, ich bin in New York, möchte Geld im Finanzwesen bewegen und muss meine Betrüger in Miami bezahlen. Sie wollen ihr Geld und schnell bezahlt werden. Ich bekomme keinen Scheck und kann weder Computer noch Laptop benutzen, weil die IP-Adresse pingt. Also gehe ich zu einem Bitcoin-Geldautomaten in New York und benutze Bargeld und ein Wegwerfhandy. So kann ich Leute bezahlen und gleichzeitig die Anti-Geldwäsche-Protokolle umgehen. Das ist Fraud“, sagte Miranda.

Pig Butchering (Schweineschlachten)

Eine weitere häufige Fraudtaktik, die von Betrügern genutzt wird, ist unter dem bildhaften Begriff „Pig Butchering“ (Schweineschlachten) bekannt. „Dabei geht es im Grunde darum, dass ein Betrüger sein Opfer metaphorisch mästet, indem er viel Zeit mit ihm verbringt, um Vertrauen aufzubauen“, sagt Dana Lawrence, Chief Compliance Officer bei der Unternehmens- und Technologieberatung Fideseo. Betrüger können laut Lawrence überall Zeit investieren, am häufigsten geschieht dies jedoch entweder in sozialen Medien oder per SMS über Wochen oder Monate hinweg. Lawrence nannte insbesondere LinkedIn sowie soziale Netzwerke wie Twitter als bevorzugte Plattform.

In diesen Fällen präsentiert sich der Betrüger typischerweise als Influencer oder Insider, der erfolgreich in Kryptowährungen investiert hat. Im Laufe der Zeit preist er die Vorteile von Kryptowährungen an, um das Opfer dazu zu bewegen, ihm sein Vermögen zu übertragen. In einigen Fällen haben Betrüger dem Opfer auch gefälschte Finanzberichte vorgelegt, um den Anschein erheblicher Gewinne zu erwecken.

Obwohl diese Anzeichen leicht zu erkennen sind, sind die Betrüger in diesem Fall äußerst raffiniert vorgegangen. Betrügerteams in Ländern wie Kambodscha und China beispielsweise wurden von Psychologen intensiv darin geschult, Menschen anfällig für unüberlegte Entscheidungen zu machen.

„Sie wurden von Psychologen darauf trainiert, herauszufinden, wie man Menschen am besten manipuliert“, sagte Jeff Rosen, Bezirksstaatsanwalt von Santa Clara County, Kalifornien, in einem CNN-Interview. „Sie haben es mit Leuten zu tun, die psychologische Techniken anwenden, Sie verletzlich machen und Sie dazu zu bringen, sich von Ihrem Geld zu trennen.“[1]

Pump and Dump

Die andere große Fraudform, die in der Kryptosphäre zu beobachten ist, ist langjährigen Beobachtern des Aktienmarktes wohlbekannt: das sogenannte „Pump and Dump“-System.

„Dieses Schema beginnt typischerweise damit, dass sich eine Gruppe zusammenschließt, um ein neues Kryptoprojekt, beispielsweise einen Token, zu starten und dann – meist mit Hilfe von Influencern – Ressourcen nutzt, um es auf Plattformen wie Twitter oder Discord zu hypen“, sagte Lawrence. „Derzeit herrscht aufgrund der Liquidität große Fluktuation auf dem Kryptomarkt. Wenn also viele Leute gleichzeitig versuchen, etwas zu kaufen, schockt das den Markt und führt zu steigenden Preisen. In diesem Fall verkaufen die Betrüger, die große Mengen des Vermögenswerts halten, diese plötzlich mit Gewinn, wodurch der Preis schlagartig sinkt und alle anderen Investoren mit etwas praktisch Wertlosem zurückbleiben.“

Das Warnsignal in solchen Fällen, so Lawrence, sei ein deutlicher Mangel an Offenlegungen, die potenziellen Investoren deutlich machen, dass ein Totalverlust durchaus möglich ist. Die Täter nutzen zudem häufig kopierte und eingefügte Nachrichten in sozialen Medien und Diskussionsforen, die von Nutzern mit ähnlichen Benutzernamen verfasst wurden. Sobald das Komplott abgeschlossen ist, verschwinden in der Regel die Benutzernamen, und die Anonymität bleibt vollständig gewahrt.

Weitere Beispiele für Fraud im Zusammenhang mit Krypto-Assets

Kryptobasierter Fraud muss nicht immer so raffiniert sein. In kryptobasierten Organisationen reicht einem Angreifer oft die richtige Gelegenheit. Während beispielsweise die Blockchain selbst digitale Vermögenswerte sichert, genügt es, sich einen privaten Schlüssel zu beschaffen, um die Sicherheitsvorkehrungen zu umgehen und eine Krypto-Wallet zu leeren – eine lange Zahlenfolge, die auf eine Restaurantserviette passt und überall für jedermann auffindbar hinterlassen werden kann.

„Ihr privater Schlüssel ist Ihre digitale Identität auf dem Kryptowährungsmarkt, und jeder, der ihn in die Hand bekommt, kann betrügerische Transaktionen durchführen oder Ihre Kryptowährungen stehlen“, sagte Lawrence. „Wenn sich jemand irgendwie Zugang dazu verschafft und alle meine Bitcoins abhebt, kann ich nichts dagegen tun. Ich kann sie nicht zurückbekommen, ich kann keine Beschwerde einreichen, es gibt keine Verbraucherschutzbehörde oder Regulierungsbehörde, bei der ich Einspruch einlegen könnte – sie sind weg.“

Mit zunehmender Reife des Kryptomarktes sind Krypto-Sicherheitsdienste entstanden, die sich auf den Schutz privater und Unternehmensschlüssel vor Verlust spezialisiert haben. Ihre Methoden sind jedoch teilweise überraschend primitiv. Laut Lawrence besteht die Lösung mancher dieser Dienste darin, die Schlüssel in Tresoren an verödeten Berghängen aufzubewahren. Krypto-Versicherungen dienen Unternehmen, die es sich leisten können, als Sicherheitsnetz. Allerdings kämpft die gesamte Branche derzeit mit der Rentabilität, was die Versicherer zu einer äußerst selektiven Vorgehensweise zwingt und gleichzeitig die Deckungssumme von Jahr zu Jahr schrumpfen lässt.

In einem Artikel in der britischen Insurance Times diskutierte James Wickes, Partner der RPC Insurance Group, die Herausforderungen des Krypto-Versicherungsmarktes. „Die relativ kleine Zahl der derzeit im Bereich der Krypto-Asset-Versicherung tätigen Versicherer dürfte das Kleingedruckte in den Policen sorgfältig prüfen, um das potenzielle Risiko der Volatilität der Kryptomärkte zu begrenzen, wie der jüngste Crash gezeigt hat“, sagte er. „Der Versicherungsmarkt für diese Vermögenswerte steckt noch in den Kinderschuhen, und es bleibt abzuwarten, ob genügend Versicherungsträger bereit sein werden, die Nachfrage zu decken, und wie mutig der Markt sein wird, den Versicherungsschutz über das traditionelle Diebstahlrisiko hinaus auszuweiten.“[2]

Trotz dieser Vorsichtsmaßnahmen gibt es jedoch weiterhin bestimmte Tools, mit denen Kriminelle Krypto-Assets und Blockchain nutzen können, ohne ein bestehendes Konto direkt zu umgehen – nämlich Mixer, auch bekannt als Tumbler. Eines der Hauptmerkmale einer Blockchain ist ihre Transparenz. In jedem Blockchain-Explorer kann jeder die Aufzeichnungen aller Blockchain-Transaktionen seit der Einführung der Kryptowährung im Jahr 2009 einsehen. Mixer ermöglichen es dem Benutzer, die Menge der betreffenden Krypto-Assets wesentlich durcheinander zu bringen, bevor sie an die vorgesehenen Empfänger übermittelt werden. Dies gewährt ihm ein gewisses Maß an

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 .

Anonymität, da es so schwierig ist, genau zu entschlüsseln, wer wie viele Assets an wen gesendet hat. Mit einem Mixer zeigt ein Explorer lediglich, dass eine Person sowie Dutzende anderer Personen Assets an einen Mixer gesendet und diese dann in unterschiedlichen Mengen an verschiedene andere Personen gesendet haben. Das Ergebnis ähnelt im Wesentlichen einer perfektionierten Form der Geldwäsche.

Angesichts dieser Realitäten müssen Organisationen, die sich für die Kryptowelt entscheiden, akzeptieren, dass sie in dieser Phase bei der Risikominimierung weitgehend auf sich allein gestellt sind. Das bedeutet nicht, dass Krypto vermieden werden sollte, aber es bedeutet, dass Compliance, solide interne Kontrolle, Frauderkennung und -abschreckung sowie Interne Revision in Diskussionen über Krypto von der Leitungsebene an abwärts eine überragende Rolle spielen müssen.

Wo die Interne Revision ansetzen kann

Die Regulierung ist da, und es wird noch mehr folgen

Veröffentlichte Leitlinien

Wie bereits erwähnt, gibt es kaum regulatorische Rahmenbedingungen für Unternehmen, um die Sicherheit und Governance von Krypto-Assets und den damit verbundenen Fraudrisiken zu gewährleisten. In bestimmten Branchen, wie beispielsweise im Finanzdienstleistungssektor, mangelt es jedoch nicht an Vorgaben, die angemessene Governance-Prinzipien für den Schutz digitaler Assets behandeln – viele davon sind auch auf Kryptowährungen anwendbar.

Im Oktober 2022 hat die Europäische Union den vereinbarten Text der Markets in Crypto-Assets (MiCA) Regulation vorgelegt. Dies ist einer der ersten Versuche weltweit, den Kryptowährungshandel umfassend zu regulieren. Die Übersetzung in 24 verschiedene Sprachen wurde jedoch bis April 2023 verschoben. Sollte die Verordnung formell verabschiedet werden, wird sie:

- Offiziell Krypto-Asset definieren als eine digitale Darstellung von Werten oder Rechten unter Verwendung von Distributed-Ledger-Technologie oder ähnlicher Technologie, die elektronisch übertragen und gespeichert werden können. Darüber hinaus gibt es vier verschiedene Kategorien von Krypto-Assets: Asset-Referenced Tokens, E-Money Tokens, Utility Tokens und eine vierte Kategorie für Krypto-Assets, die nicht in die anderen drei Kategorien fallen.
- Krypto-Anbieter offiziell haftbar machen, wenn sie die Krypto-Vermögenswerte der Anleger verlieren.
- Von den Akteuren auf den Märkten für Krypto-Assets verlangen, Informationen zu ihrem ökologischen und klimatischen Fußabdruck offenzulegen.
- Sich mit der aktualisierten Gesetzgebung zur Bekämpfung der Geldwäsche überschneiden und die Europäische Bankenaufsichtsbehörde (EBA) wird mit der Führung eines öffentlichen Registers nicht konformer Anbieter von Krypto-Asset-Diensten beauftragt.
- Von Anbietern von Krypto-Assets eine Zulassung für den Betrieb in der EU verlangen.
- Einen starken Rahmen für „Stablecoins“ (Kryptowährungen, die an einen externen Referenzwert gekoppelt sind) schaffen, der vorsieht, dass jeder Stablecoin-Inhaber beim Emittenten jederzeit kostenlos einen Anspruch hat.[3]

In den USA bietet eine gemeinsame Erklärung der Federal Reserve, der Federal Deposit Insurance Corporation (FDIC) und des Office of the Comptroller of the Currency (OCC) US-Unternehmen einige Ressourcen mit Leitlinien, die Bankorganisationen dabei helfen sollen, sich an intensiven Aufsichtsdiskussionen über geplante und bestehende Aktivitäten im Zusammenhang mit Krypto-Assets zu beteiligen.[4] Dazu gehören:

- OCC Interpretataive 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 .

Dies sind jedoch nicht die einzigen verfügbaren Ressourcen. Nach dem Zusammenbruch von FTX veröffentlichte die SEC zudem Richtlinien, in denen Unternehmen dazu angehalten wurden, ihre Beteiligung an Unternehmen im Bereich digitaler Rohstoffe offenzulegen.

Der Wert der Bildung

Vorausgesetzt sie wird angenommen, würde die vorgeschlagene EU-Gesetzgebung 2024 in Kraft treten, aber mit ziemlicher Sicherheit nicht die letzte sein. Da sich das Patchwork der Regulatorik jeden Monat mehr füllt, ist es für einen internen Revisor äußerst wichtig, sich über Änderungen auf dem Laufenden zu halten und diese dem Leitungsorgan und den relevanten Stakeholdern klar zu kommunizieren.

Im aktuellen Umfeld sollten Revisoren den Stakeholdern auch klarmachen, welche weiteren Vorschriften für Krypto-Aktivitäten gelten könnten. Beispielsweise, so Lawrence, müsse sich ein Unternehmen, das eine eigene Kryptowährung anbietet, möglicherweise beim US Financial Crimes Enforcement Network registrieren lassen – ein wichtiges Detail, das leicht übersehen werden könne, da Kryptowährungen in der Gesetzgebung nicht explizit erwähnt werden. „Es herrscht derzeit große Unsicherheit", sagte sie. „Es liegt an den Revisoren, die Führungskräfte darüber zu informieren, was anwendbar ist und was nicht."

Der Fokus auf neue Technologien sollte Unternehmen auch nicht von grundlegenden Best Practices zum Schutz digitaler Vermögenswerte ablenken, einschließlich der Nutzung eines virtuellen privaten Netzwerks (VPN) und der ordnungsgemäßen Sicherung, Erfassung und gegebenenfalls Löschung von Benutzerprofilinformationen – insbesondere von Verbrauchern. „Benutzerprofile sind eine wichtige organisatorische Kontrolle", sagte Miranda. „Wenn ich ein Unternehmen prüfen würde, würde ich sicherstellen, dass die Benutzerprofile mit den Transaktionsaktivitäten übereinstimmen. Beispielsweise sind geografische Informationen für Compliance und Ermittlungen unglaublich wichtig. Unternehmen müssen diese Informationen sicher aufbewahren und wissen, wo sie gespeichert sind." In diesem Zusammenhang merkte Miranda an, dass Unternehmen häufig Geheimhaltungsvereinbarungen (NDAs) übersehen, die wichtige Profilinformationen wie Postanschriften enthalten, die für eine Fraudermittlung von entscheidender Bedeutung sein können.

Für weitere Informationen bietet „Interne Revision und Fraud: Beurteilung von Fraudrisiko-Governance und -Management auf Ebene der Organisation" im Bereich der Ergänzenden Leitlinien des IIA klare Anweisungen zu den organisatorischen Rollen und Verantwortlichkeiten für solides Fraudrisiko-Governance und -Management sowie Empfehlungen für zusätzliche Anleitungen wie den Fraudrisiko-Management-Leitfaden von COSO.

Fazit

Die Interne Revision ist bereit

Kryptowährung und die Technologie, auf der sie basiert sind zu revolutionär, als dass die interne Revision sie ignorieren könnte, da die Risiken die Aufmerksamkeit des Leitungsorgans mehr als verdienen. Risikobeurteilungen, die dies ignorieren, haben einen kritischen blinden Fleck. Kryptowährungen mögen für viele ein relativ neues Konzept sein, mindern jedoch nicht den Wert eines soliden Rahmens für das Fraudrisikomanagement, der von der Internen Revision gemessen und getestet werden kann.

Es ist leicht, ein zusätzliches Risikofeld auf dem immer größer werdenden Radar der Internen Revision zu beklagen. Die gute Nachricht ist jedoch, dass keine andere Abteilung besser aufgestellt ist, um dieses Problem anzugehen. Ähnlich wie der Sarbanes-Oxley Act (SOX) im Jahr 2002 sichert die Weiterentwicklung der Kryptowährungsregulierung der Internen Revision für Jahre einen wertvollen Platz am Tisch. Auch wenn die Revision noch keine Kryptowährungen kennt, kennt sie Fraud und Risiken. Das allein reicht aus, um die Interne Revision in die Lage zu versetzen, eine führende Position bei der Bewältigung der bevorstehenden Herausforderungen einzunehmen.

Teil 2

Interne Revision und Fraudermittler: Eine wertvolle Partnerschaft

Über die Experten

Mason Wilder, CFE

Mason Wilder ist zertifizierter Fraudermittler und Forschungsleiter bei der ACFE. In dieser Funktion beaufsichtigt er die Erstellung und Aktualisierung von ACFE-Materialien für die berufliche Weiterbildung, unterstützt die Planung und Durchführung aller ACFE-Schulungsveranstaltungen, arbeitet an Forschungsinitiativen wie dem „Report to the Nations“ und Benchmarking-Berichten, leitet Schulungen, schreibt für ACFE-Publikationen und beantwortet Anfragen von Mitgliedern und Medien. Vor seinem Eintritt bei der ACFE war Wilder über ein Jahrzehnt im Bereich Unternehmenssicherheitsinformationen und -ermittlungen tätig und spezialisierte sich auf Hintergrund- und Due-Diligence-Untersuchungen sowie Geheimdienstanalysen für die internationale physische Sicherheit und Krisenreaktion. Mason hat seine Karriere darauf aufgebaut, relevante Informationen aus allen Quellen zu sammeln, um sie zur Unterstützung kritischer Entscheidungen zu analysieren und zu verarbeiten. Es ist ihm ein Herzensanliegen, Experten in der Fraudbekämpfung dabei zu unterstützen, ihre Fähigkeiten zur effektiven Fraudbekämpfung kontinuierlich zu verbessern.

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

Shawna Flanders, Leiterin der Produktentwicklung beim Institute of Internal Auditors (IIA), ist eine leidenschaftliche Technologin und Fachkraft in der Branche fachlicher Schulungen. Ihre Leidenschaft gilt der Übertragung technischer Konversationen in die gängige Geschäftssprache. Shawna bringt in jeden Auftrag eine einzigartige, sich ergänzende Kombination von Fähigkeiten ein, darunter: Entwicklung/Beitrag von KMU-Inhalten, Vortrag/Schulung, IT-bezogene Risiken, IT-Audit, Informations- und Cybersicherheit, IT-Compliance, IT-Governance, Lieferantenmanagement, IT-Generalist in der Telekommunikation, Programmierung, Konzeption/Überprüfung sprach- und datenbezogener Architekturen, Engineering, Analyse- und Integrationsmanagement, Geschäftsprozessmanagement, Geschäftsanalyse, Projektmanagement, Programmmanagement und Prozessverbesserung/Six Sigma.

Einleitung

Interne Revisoren liefern konstruktive Einblicke zu Governance, Risiken und internen Kontrollen, die Unternehmen beim Risikomanagement unterstützen, einschließlich der Erkennung und Eindämmung von Fraud. Die Interne Revision ist zwar ein wirksamer Bestandteil der Frauderkennung und -abwehr, die Aufdeckung von Fraud ist jedoch nicht ihre Aufgabe. Ein Certified Fraud Examiner (CFE) hingegen ist speziell mit der Erkennung und Untersuchung von Fraudfällen beauftragt. Der CFE bringt spezielle Fähigkeiten in den Kampf gegen Fraud ein. Daher ist es sinnvoll, dass beide Berufsgruppen im besten Interesse der Organisation zusammenarbeiten.

Dieser Global Knowledge Brief, der zweite einer dreiteiligen Reihe zum Thema Fraud, untersucht die Vorteile des Aufbaus einer symbiotischen Beziehung zwischen Internen Revisoren und CFEs.

Das Ausmaß von Fraud

Durchschnittlicher Verlust fast 1,8 Millionen US-Dollar

Fraud bleibt ein allgegenwärtiges Risiko

Fraud ist jede illegale Handlung zum finanziellen oder persönlichen Vorteil, die Täuschung, Verschleierung oder Vertrauensbruch beinhaltet. Personen oder Organisationen, die Fraud begehen, versuchen, Geld, Eigentum oder Dienstleistungen zu stehlen, die Zahlung oder den Verlust von etwas zu vermeiden oder sich einen persönlichen oder geschäftlichen Vorteil zu verschaffen. Neben externen Betrügern können auch Mitarbeiter, die unter finanziellem Druck stehen oder der Meinung sind, dass ihnen das Geld oder die in Anspruch genommenen Dienstleistungen zustehen, weil sie sich ungerecht behandelt fühlen oder ein anderer Grund für Fraud vorliegt, Fraud begehen. Jede Organisation kann Opfer von Fraud werden, unabhängig von ihrer Größe und davon, ob es sich um eine öffentliche, private oder gemeinnützige Organisation, eine Regierungsbehörde, ein öffentliches oder privates Versorgungsunternehmen oder eine andere Einrichtung handelt.

Fraud stellt für Unternehmen ein ernstzunehmendes und weit verbreitetes Risiko dar. Die Folgen von Fraud können von schwerwiegend bis verheerend reichen. Dazu gehören nicht nur finanzielle Herausforderungen und Verluste, sondern auch Ineffizienzen, die den Betrieb, den Umsatz oder den Gewinn beeinträchtigen, die Absage von Projekten und, je nach Ausmaß, möglicherweise der Zusammenbruch der Organisation.[5]

Eine weltweite Umfrage der Association of Certified Fraud Examiners (ACFE) unter CFEs ergab 2.110 Fraudfälle in 133 Ländern. Innerhalb dieser Gruppe beliefen sich die weltweiten Verluste durch Fraud auf über 3,6 Milliarden US-Dollar, wobei der durchschnittliche Verlust pro Fall bei knapp 1,8 Millionen US-Dollar lag. CFEs schätzen, dass Unternehmen jährlich 5 % ihres Umsatzes durch Fraud verlieren. Kleinere Unternehmen waren dabei eindeutig dem größten Fraudrisiko ausgesetzt: Unternehmen mit der kleinsten Belegschaft erlitten mit 150.000 US-Dollar den höchsten Verlustmedian.

Verluste dieser Größenordnung sind leicht zu erkennen, aber Fraud geschieht oft in kleineren Schritten über einen längeren Zeitraum. Ein typisches Fraudschema kann laut der Umfrage zu einem Verlust von 8.300 Dollar pro Monat führen und bis zur Aufdeckung 12 Monate dauern. Wichtig zu wissen ist auch, dass Kryptowährungen nach Feststellung der ACFE in 8 % der Fälle involviert sind. Zu den üblichen Szenarien gehörten Bestechungs- und Schmiergeldzahlungen sowie die Veruntreuung von Vermögenswerten.[6]

Kategorien von Fraud im beruflichen Umfeld

Laut ACFE 2022 Report to the Nations gibt es drei Hauptkategorien von beruflichem Fraud.

Fraudmethoden in der Finanzberichterstattung oder das Verursachen einer wesentlichen Falschdarstellung oder Auslassung in den Finanzberichten der Organisation waren am seltensten (9 %), aber mit einem Verlust von 593.000 US-Dollar pro Fall auch die teuersten.

Veruntreuung von Vermögen, bei der ein Mitarbeiter Unternehmensressourcen stiehlt oder missbraucht. Allerdings war dieser Fall für die geringsten durchschnittlichen Verluste verantwortlich: 100.000 US-Dollar pro Fall.

Korruption, die Bestechung, Interessenkonflikte und Erpressung umfasst, war in 50 % der Fälle im Spiel und führte zu Verlusten von 150.000 US-Dollar pro Fall.

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

[5] 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..

Die Rolle des Internen Revisors

Prüfungssicherheit und Beratung zur Fraudprävention

Frauderkennung und Fraudabschreckung als tragende Säule der Internen Revision

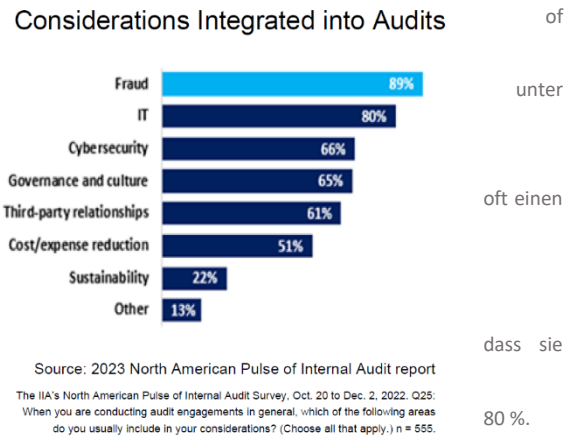
Laut dem Institute of Internal Auditors (IIA) ist „die interne Revision eine unabhängige, objektive Prüfungs- und Beratungsfunktion, die darauf abzielt, Mehrwert zu schaffen und die Geschäftsabläufe einer Organisation zu verbessern. Ihre Aufgabe umfasst die Erkennung, Prävention und Überwachung von Fraudrisiken sowie die Berücksichtigung dieser Risiken in Prüfungen und Untersuchungen."[7]

Organisationen sollten nicht erwarten, dass die Interne Revision auch Fraudermittlungen durchführen kann. Wenn die Umstände es erfordern, dass die Interne Revision eine Ermittlungsfunktion übernimmt, sollten die Internen Revisorinnen und Revisoren die gebotene professionelle Sorgfalt walten lassen und nur tätig werden, wenn sie über die erforderliche Erfahrung und Expertise verfügen.

Während die Fraudprävention Aufgabe des Managements ist, unterstützt die Interne Revision die Fraudbekämpfung, indem sie die notwendigen Prüfungsleistungen für interne Kontrollen zur Aufdeckung und Verhinderung von Fraud erbringt. Fraud entsteht häufig aufgrund von schlecht konzipierten Kontrollen und einer schwachen Governance, die die Prozesse des Unternehmens untergräbt. Fast die Hälfte der Fälle in der ACFE-Umfrage war auf fehlende interne Kontrollen (29 %) oder die Außerkraftsetzung bestehender Kontrollen (20 %) zurückzuführen. Prüfer berücksichtigen das Fraudpotenzial und die Angemessenheit der internen Kontrollen in den von ihnen untersuchten Bereichen. Laut der Umfrage sind durch Anti-Fraudkontrollen tendenziell geringere Verluste durch Fraud und eine schnellere Aufdeckung von Fraudfällen möglich.

Der Beitrag der Internen Revision zur Fraudbekämpfung sollte nicht unterschätzt werden. Als das IIA die Revisionsleitungen (CAE) bat, anzugeben, worin die Interne Revision maßgeblich beteiligt ist, nannten 57 % Fraud und 56 % die allgemeine Risikobeurteilung.[8] Die ACFE-Umfrage ergab inzwischen, dass der durchschnittliche Schaden durch Fraud um 50 % höher war (150.000 US-Dollar gegenüber 100.000 US-Dollar), wenn keine Interne Revision vorhanden war.

Tatsächlich zeigen Daten aus dem kommenden North American Pulse Internal Audit Report 2023, dass Fraud die am häufigsten genannte Risikoüberlegung in internen Prüfungen ist. In der jährlichen Umfrage nordamerikanischen Revisionsleitungen wurden mehr als 500 Teilnehmer gebeten, anzugeben, welche Bereiche sie generell in ihre Prüfungen einbeziehen. „Die Antworten deuten darauf hin, dass Prüfer ganzheitlichen Ansatz verfolgen und ein breites Spektrum an Themen berücksichtigen, darunter Cybersicherheit, Drittparteien und Governance", heißt es in dem Bericht, der im März auf der GAM Conference 2023 vorgestellt wird. Insgesamt gaben 89 % der CAEs an, generell in jede Prüfung Fraudüberlegungen einbeziehen, die am häufigsten genannte Risikokategorie, gefolgt von IT-Überlegungen mit



of unter oft einen dass sie 80 %.

Laut dem IIA-Positionspapier zu *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*[9] sollte die Interne Revision über die erforderlichen Kenntnisse zum Thema Fraud verfügen, um in der Lage zu sein:

- Warnsignale (red flags) zu erkennen, die auf Fraud hindeuten könnten.

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

- die Merkmale von Fraud und die Techniken zur Begehung von Fraud sowie die Arten von Fraudschemata und -szenarien zu verstehen.
- entscheiden können, ob weitere Maßnahmen erforderlich sind oder ob eine Untersuchung empfohlen werden sollte.
- die Wirksamkeit von Kontrollen zur Verhinderung oder Aufdeckung von Fraud zu bewerten und Verbesserungsmöglichkeiten zu identifizieren.

Die Rolle des Fraudermittlers

Untersuchung von Täuschungen

Kompetente Fraudermittlungen sind entscheidend

Der Fraudermittler beteiligt sich und unterstützt die allgemeinen Programme zur Aufklärung von Fraud in der Organisation. Dies geschieht unter anderem durch Fraudermittlungen, die darauf abzielen, „Fakten und Beweise zu sammeln, um den Vorfall aufzuklären, die verantwortliche Partei zu identifizieren und gegebenenfalls Empfehlungen abzugeben".[10] Eines der Probleme, die ein Prüfer bei der Einleitung einer Untersuchung berücksichtigt, ist *die Prädikation.* Das bedeutet, dass die Gesamtheit der Umstände es für einen gut ausgebildeten Fachmann plausibel erscheinen lassen muss, dass Fraud stattgefunden hat.

Zu den Schritten, die ein Fraudermittler im Rahmen einer Untersuchung unternimmt, gehören unter anderem die Beschaffung von Beweismitteln, die Berichterstattung über die Ergebnisse, die Abgabe von Zeugenaussagen zu den Ergebnissen sowie die Unterstützung bei der Aufdeckung und Prävention von Fraud. Zwei gängige Zwecke einer Frauduntersuchung sind die Untersuchung eines potenziellen Fraud oder Fraudvorwurfs und die Überprüfung der Fraudbekämpfungsrichtlinien und -kontrollen eines Unternehmens. Konkretere Ziele einer Frauduntersuchung können sein:

- Erkennen von Fehlverhalten, das mit Fraud in Verbindung steht oder stehen könnte, sowie Feststellen, wer für etwaiges Fehlverhalten verantwortlich ist.
- Ermittlung der tatsächlichen oder potenziellen Verluste oder Verbindlichkeiten aus einem Fraudfall.
- Das Engagement der Organisation demonstrieren, Fraud zu erkennen und einzudämmen.
- Helfen, die Schadensregulierung zu erleichtern.
- Verhindern künftiger Fraudfälle und damit verbundener Verluste oder Verbindlichkeiten.
- Handhabung der Folgen, die über finanzielle Verluste hinausgehen.
- Auffinden und Beheben von Schwachstellen in internen Kontrollen.
- Falls zutreffend, die Einhaltung von Gesetzen, Vorschriften, Verträgen oder gewohnheitsrechtlichen Pflichten.[11]

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

Vergleich der Ansätze

Diese Tabelle zeigt einen Überblick über einige wichtige Unterschiede zwischen den Aufgaben, Ansätzen und Zielen von Internen Revisoren und CFEs.

Eigenschaften	**Interne Revision**	**Frauduntersuchung**
Absicht	Die Verfahren der Internen Revision können Fraud aufdecken, garantieren aber nicht, dass er entdeckt wird. Beispielsweise können Prüfer bei einer Prüfung eine verdächtige Transaktion oder Situation feststellen, die letztlich als Fraud identifiziert werden kann. Die Aufdeckung von Fraud ist jedoch nur ein Aspekt einer umfassenderen Untersuchung der Kontrollen und Verfahren des Prüfungsgegenstands.	Bei einer Frauduntersuchung geht es direkt darum, Fraud aufzudecken und Maßnahmen oder Aktivitäten zur Fraudbekämpfung in Betracht zu ziehen.
Auftreten	Prüfungen werden normalerweise regelmäßig wiederholt, es können jedoch auch Popup-Audits verwendet werden, um eine einzigartige Situation oder Fragestellungen in einem Bereich zu behandeln.	Frauduntersuchungen werden in der Regel nur bei ausreichender Prädiktion durchgeführt, können aber auch ohne konkreten Anlass im Rahmen eines Risikomanagement- oder Fraudrisikobeurteilungsprogramms erfolgen. Die meisten Fraudfälle werden jedoch aufgrund von Hinweisen oder Vorwürfen durchgeführt. Die ACFE-Umfrage ergab, dass 43 % der Fraudfälle aufgrund von Hinweisen aufgedeckt wurden – fast dreimal so häufig wie bei der nächsthäufigsten Methode zur Fraudaufdeckung. Mehr als die Hälfte aller Fraudhinweise kam von Mitarbeitern.
Konfrontativ oder nicht?	Revisionsprüfungen sind nicht konfrontativ. Ziel der Prüfer ist es, Erkenntnisse und Informationen zu liefern, die Teamleiter und -mitglieder beispielsweise zur Verbesserung von Kontrollen oder anderen Prozessen nutzen können.	Fraudermittlungen sind grundsätzlich konfrontativ. Ziel ist es unter anderem, die Schuld desjenigen nachzuweisen, der Fraud begangen hat.
Standards	Interne Revisoren befolgen die *International Standards for the Professional Practice of Internal Auditing*, die vom Institute of Internal Auditors (IIA) festgelegt wurden.	CFEs befolgen den ACFE *Code of Professional Standards* . CFEs können bei ihren Untersuchungen ein ACFE-Tool zur Fraudrisikobeurteilug verwenden.

Zusammenarbeit zum Erfolg führen

Gegenseitiger Respekt und Verantwortung

Im Kampf gegen Fraud

Es gibt zahlreiche Möglichkeiten für eine gewinnbringende Zusammenarbeit zwischen Revisoren und Fraudermittlern. Sie können sich über Folgendes beraten:

- Einleitung einer Fraduntersuchung.
- Jährliche Planung von Prüfungen und Frauduntersuchungen.
- Risikobewertungen.
- Evaluierung und Beurteilung von Kontroll- und Fraudbekämpfungsprogrammen.
- Übermittlung von Prüfungsergebnissen mit Auswirkungen auf Fraud.
- Behebung von Kontrollschwächen.

Viele Organisationen haben Regeln für die Abläufe, wenn die Interne Revision einen Fraudfall an ein externes oder internes Fraudermittlungsteam weiterleitet. Das Revisionsteam nimmt den Fraudfall zur Kenntnis und erstellt am Ende der Überprüfung gemeinsam mit dem Fraudermittler einen Bericht.

Darüber hinaus kann die Interne Revision die Fraudbekämpfungsabteilung einer Organisation prüfen, um sicherzustellen, dass deren eigenen Kontrollen angemessen sind. Ein Fraudbekämpfungsteam kann der Rechtsabteilung oder dem Risikomanagementteam der Organisation oder anderen Bereichen, einschließlich der Internen Revision, unterstellt sein. Falls ein Fraudbekämpfungsteam der Internen Revision unterstellt ist, sollte die Prüfung dieser Abteilung ausgelagert werden, um Objektivität zu gewährleisten.

Eine Fallstudie zur Veranschaulichung der Zusammenarbeit am Arbeitsplatz

Die folgende Fallstudie zeigt, wie die beiden Teams zusammenarbeiten können. Sie basiert auf einer von Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB, Leiterin der Produktentwicklung beim IIA, geführten Diskussion in einem aktuellen IIA- und ACFE-Webinar zum Thema *„Förderung der Zusammenarbeit: Der Revisor und der Fraudermittler“.*

Normalerweise entdeckt die Interne Revision ein Muster, das auf Fraud hindeutet, und alarmiert die Fraudermittler. Im von Flanders vorgestellten Fall umfasste die Interne Revision eine Überprüfung von Autokrediten. Das Team untersuchte unter anderem überfällige Konten. Unter 40 solcher Konten fielen fünf auf. Das System war so eingestellt, dass es überfällige Kredite, die einer Überprüfung bedurften, markierte, doch aus unerfindlichen Gründen wurden diese fünf nicht markiert. Zudem wiesen sie alle ungewöhnliche Merkmale auf: einen Zinssatz von 0 %, eine Laufzeit von 72 Monaten und keine Mindestzahlung.

Bei ihren Nachforschungen stellte Flanders fest, dass die mit den Krediten verknüpfte Benutzer-ID einem Kundendienstmitarbeiter gehörte. Das ergab keinen Sinn. Normalerweise genehmigte niemand in dieser Funktion Kredite. Anschließend überprüfte sie die Protokolldateien der Kredite und stellte fest, dass dem Inhaber der Benutzer-ID etwa eine Stunde vor der Einreichung und Genehmigung jedes Kredits zusätzlicher Zugriff auf das System gewährt wurde. Dieser Zugriff wurde etwa eine Stunde nach Genehmigung und Aktivierung der Kredite wieder entzogen. Angesichts der ungewöhnlichen Kreditbedingungen, der Beteiligung eines Kundendienstmitarbeiters und der Änderungen beim Systemzugriff wusste das Prüfteam, dass es an der Zeit war, den Fall an die Fraudabteilung des Unternehmens zu übergeben.

Abhängig von den Richtlinien und Verfahren der Organisation kann die Fraudabteilung in diesem Fall folgende Schritte unternehmen, wenn sie auf die verdächtige Aktivität aufmerksam gemacht wird:

- Bestätigung der von den Prüfern übermittelten Informationen.

- Untersuchung des gesamten Umfangs der Aktivitäten im Zusammenhang mit diesen Konten.
- Feststellung, ob die Erstellung dieser fünf Konten eine einmalige Aktion oder Teil eines potenziell laufenden Plans war.
- Identifikation aller an der Konspiration Beteiligten.
- Überlegung, ob andere Zweigstellen oder Standorte sind und welches Ausmaß der Fraud insgesamt hat.

Die Fraudermittler könnten an diesem Punkt auch überlegen, ob und wie der Fraud gestoppt werden sollte. Werden weitere Beweise oder Informationen benötigt, kann entschieden werden, den Fraud zumindest vorübergehend fortzusetzen. Diese Entscheidung ist komplex und hängt davon ab, wie viel das Unternehmen bereits verloren hat und wie viel potenziell verloren gehen könnte, wenn der Fraud fortgesetzt wird, sowie von der Risikobereitschaft des Unternehmens, so Mason Wilder, CFE, Forschungsleiter bei der ACFE, der ebenfalls am Webinar teilnahm. In diesem Fall könnten die Schritte vor der Einstellung des Fraud die Befragung des Kundendienstmitarbeiters umfassen, um weitere Informationen zu erhalten, das Ausmaß des Fraud zu ermitteln und möglicherweise weitere Fraudfälle oder Pläne für weitere Fraudfälle aufzudecken.

Sobald die Fraudermittler Beweise gesammelt und analysiert haben, berichten sie ihre Ergebnisse mündlich oder schriftlich an die zuständigen Personen im Unternehmen. Dies kann beispielsweise das Management, ein Leitungsorgan oder ein Prüfungsausschuss sein. „Ein Frauduntersuchungsbericht ist eine Beschreibung der spezifischen Aktivitäten, Ergebnisse und gegebenenfalls Empfehlungen des Fraudermittlers“, heißt es im *ACFE Fraud Examiners Manual.* Das Management der Organisation kann den Bericht nutzen, um die nächsten Schritte festzulegen.

Wenn die Fraudermittler den Fall prüfen, keinen tatsächlichen Fraud feststellen, aber feststellen, dass das Warnsignal auf einen Mangel bei den Kontrollen des Fraudrisikomanagements zurückzuführen ist, können sie den Fall zurückgeben. Die Interne Revision könnte diesen Mangel dann in ihren Bericht aufnehmen.

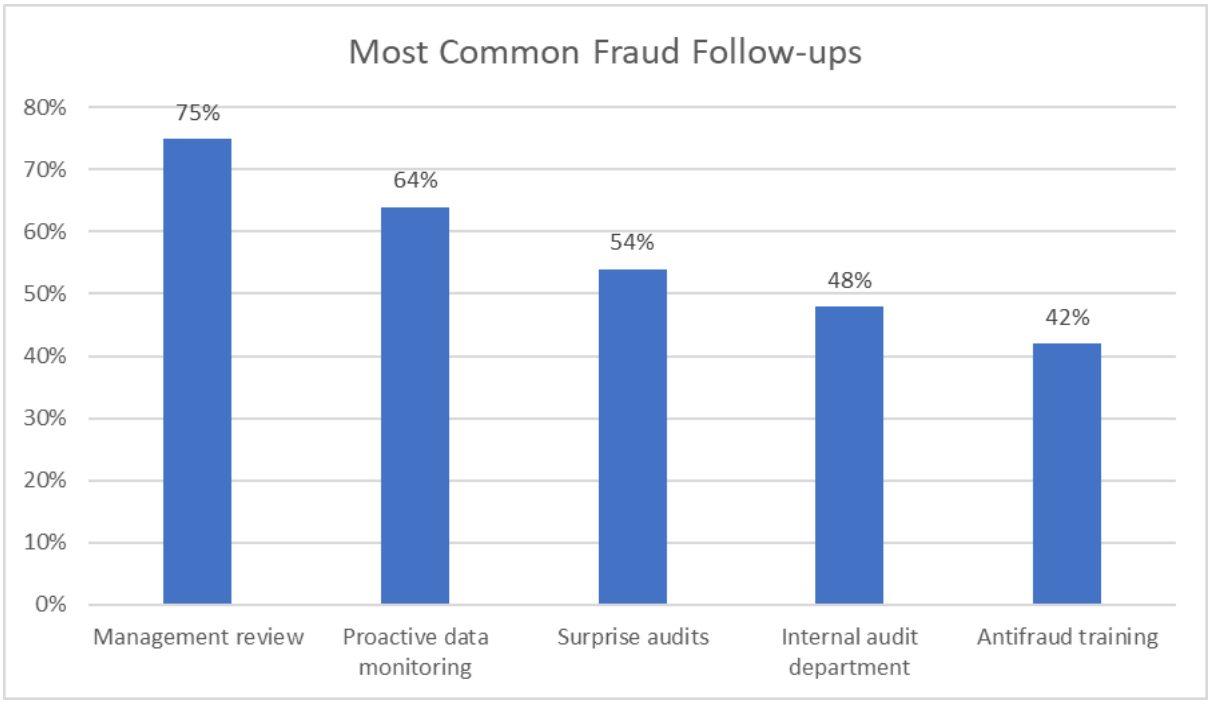
Stärken bündeln

Wer sich mit Fraud befasst, sollte bedenken, dass Schadensbegrenzung wichtig ist. Der ACFE-Umfragebericht stellte fest, dass proaktive Maßnahmen zur Frauderkennung zu einer früheren Entdeckung und geringeren Verlusten führen können, während reaktive Maßnahmen dazu führen, dass die Fraudmethoden länger andauern und die finanziellen Auswirkungen für das Opfer erhöhen.

Organisationen können jedoch nicht alle Fraudrisiken erkennen oder ausschließen. Sie sind mit zahlreichen Fraudarten, unterschiedlichen Motiven und einer breiten Palette von Tätern konfrontiert. Je besser die Mitarbeiter auf allen Ebenen – Management, Leitungsorgane und Mitarbeiter – informiert sind, desto besser können sie angemessene Maßnahmen zur Fraudbekämpfung ergreifen und Fraud bzw. die entsprechenden Warnsignale erkennen. Durch die Kombination ihrer einzigartigen Fähigkeiten und Erfahrungen können Interne Revisoren und Fraudermittler einen wichtigen Beitrag zu den Gesamtbemühungen der Organisation leisten. Organisationen können diese Arbeit nutzen, um fundiertere Entscheidungen über Fraudrisikomanagement-Ansätze zu treffen.

Schritte zur Vorbeugung eines erneuten Auftretens

Insgesamt 81 % der an der ACFE-Umfrage teilnehmenden Organisationen nahmen nach einem Fraudfall Anpassungen an ihren Fraudbekämpfungsmaßnahmen vor. Die folgende Grafik zeigt die gängigsten Maßnahmen, die von Organisationen umgesetzt oder modifiziert wurden. Weitere von der ACFE empfohlene Maßnahmen zur Fraudbekämpfung umfassen die automatisierte Transaktions-/Datenüberwachung, Beobachtung und den Kontoabgleich.



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

Fazit

Die Rolle der Internen Revision in der dritten Linie als Lieferant von Prüfungssicherheit über Governance, Risiko und interne Kontrollen erfordert Strukturen, Prozesse und Praktiken, die eine objektive und unabhängige Prüfung ermöglichen. Wie im Drei-Linien-Modell des IIA erwähnt, bedeutet Unabhängigkeit jedoch nicht Isolation.

„Es muss ein regelmäßiger Austausch zwischen Interner Revision und dem Management stattfinden, um sicherzustellen, dass die Arbeit der Internen Revision relevant und auf die strategischen und operativen Bedürfnisse der Organisation abgestimmt ist. Durch all ihre Aktivitäten baut die Interne Revision ihr Wissen und Verständnis über die Organisation auf, was zu der Prüfungssicherheit und Beratung beiträgt, die sie als vertrauenswürdiger Berater und strategischer Partner liefert“, heißt es in dem Modell.

Dies ist eindeutig der Fall, wenn die Interne Revision und zertifizierte Fraudermittler eine gemeinsame Basis als Verbündete im Kampf gegen Fraud finden.

Teil 3

Nachwirkungen: Fraud in der Nach-COVID-Zeit

Über den Experten

David Dominguez, CIA, CRMA, CPA, CFE

David ist Leiter der Abteilung Revision und Compliance bei Itafos in Houston. Im Laufe seiner Karriere hat David mit multinationalen Unternehmen verschiedener Branchen zusammengearbeitet, um unternehmensweite und regionale Revisionsfunktionen aufzubauen, zu leiten und umzugestalten. Er leitete und führte Finanz-, Betriebs- und IT-Prüfungs- und Beratungsprojekte in Nordamerika, Lateinamerika, Europa und Asien. Darüber hinaus leitete und beteiligte er sich an zahlreichen länderübergreifenden Ermittlungen, Datenanalyseinitiativen und einer Vielzahl von internationalen Aktionärs-, Joint- Venture- und Lieferantenprüfungen. Zu seinen Fachgebieten gehören Unternehmens- und Organisations-Governance, Enterprise Risk Management, Fraudrisikomanagement, der Sarbanes-Oxley Act von 2002 sowie Ethik- und Compliance-Programme.

Einleitung

Fast zwei Jahre lang verursachte COVID-19 Störungen auf allen Ebenen, angefangen bei der Arbeitsweise der Mitarbeiter und dem Ort ihrer Tätigkeit bis hin zum Umgang ihrer Organisationen mit Lieferanten und Lieferkettenproblemen und der Art und Weise, wie sie mit wichtigen Anliegen umgingen, wie etwa der Aufrechterhaltung interner Kontrollen und der Aufdeckung und Verhinderung von Fraud.

Heute atmet die Welt auf, da das Schlimmste der Pandemie langsam der Vergangenheit angehört. Dennoch sollte man nicht davon ausgehen, dass die mit COVID-19 verbundenen Risiken kein Problem mehr darstellen. Unternehmen, die von dieser Annahme ausgehen, könnten einen schwerwiegenden Fehler begehen. Dieser Global Knowledge Brief, der dritte Teil einer dreiteiligen Fraudserie des Institute of Internal Auditors (IIA), untersucht verschiedene pandemiebedingte Fraudfaktoren, die im *ACFE Report to the Nations 2022 identifiziert wurden,* ihre möglichen Auswirkungen auf Unternehmen und die Rolle der Internen Revision bei den Bemühungen der Unternehmen, diese Fraudrisikofaktoren zu mindern.

Fraud und Fraudrisiken bleiben bestehen

Pandemiebedingte Veränderungen geben weiterhin Anlass zur Sorge

Neue, von COVID inspirierte Fraudfälle werden auftauchen

In ihrem jüngsten *Report to the Nations* über Fraud im beruflichen Umfeld stellte die Association of Certified Fraud Examiners (ACFE) fest, dass die mittlere Dauer der Fraudfälle – also die typische Zeitspanne zwischen dem Beginn eines Fraud und seiner Entdeckung – 12 Monate betrug.[12] Das bedeutet, dass Unternehmen weiterhin mit pandemiebedingten Fraudfällen konfrontiert sind, die noch nicht entdeckt wurden.

Es gibt viele Gründe, warum pandemiebedingte Veränderungen das Fraudrisiko weiterhin beeinflussen. So war beispielsweise die Einführung von Homeoffice als vorübergehende Maßnahme gedacht, hat sich aber in vielen Unternehmen zum Standardverfahren entwickelt. Die Arbeit im Homeoffice brachte oft erhebliche Änderungen – und in einigen Fällen auch Lockerungen – von Praktiken und Verfahren zur Frauderkennung und -eindämmung mit sich. Daher stellen die damit verbundenen Risiken auch nach Abklingen der pandemiebedingten Störungen weiterhin eine Bedrohung für Unternehmen dar.

Die Interne Revision spielt in Schlüsselrolle – und wird sie auch künftig innehaben – bei der Bewältigung der anhaltenden Fraudrisiken im Zusammenhang mit der Pandemie. In einer von der Internal Audit Foundation (IAF) und Kroll weltweit durchgeführten Studie unter IIA-Mitgliedern waren viele Teilnehmer der durchgeführten Roundtable-Gespräche der Meinung, dass die Pandemie „der Internen Revision zu einer stärkeren Rolle beim Fraudrisikomanagement verholfen hat“.[13] Dazu gehören eine stärkere Einbindung in strategische Überlegungen zu operativen Herausforderungen, die Lieferung kontinuierlicher Prüfungssicherheit und eine verstärkte Zusammenarbeit zwischen den Geschäftsfunktionen – und das alles bei gleichzeitiger Wahrung der Unabhängigkeit der Prüfer.

[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.

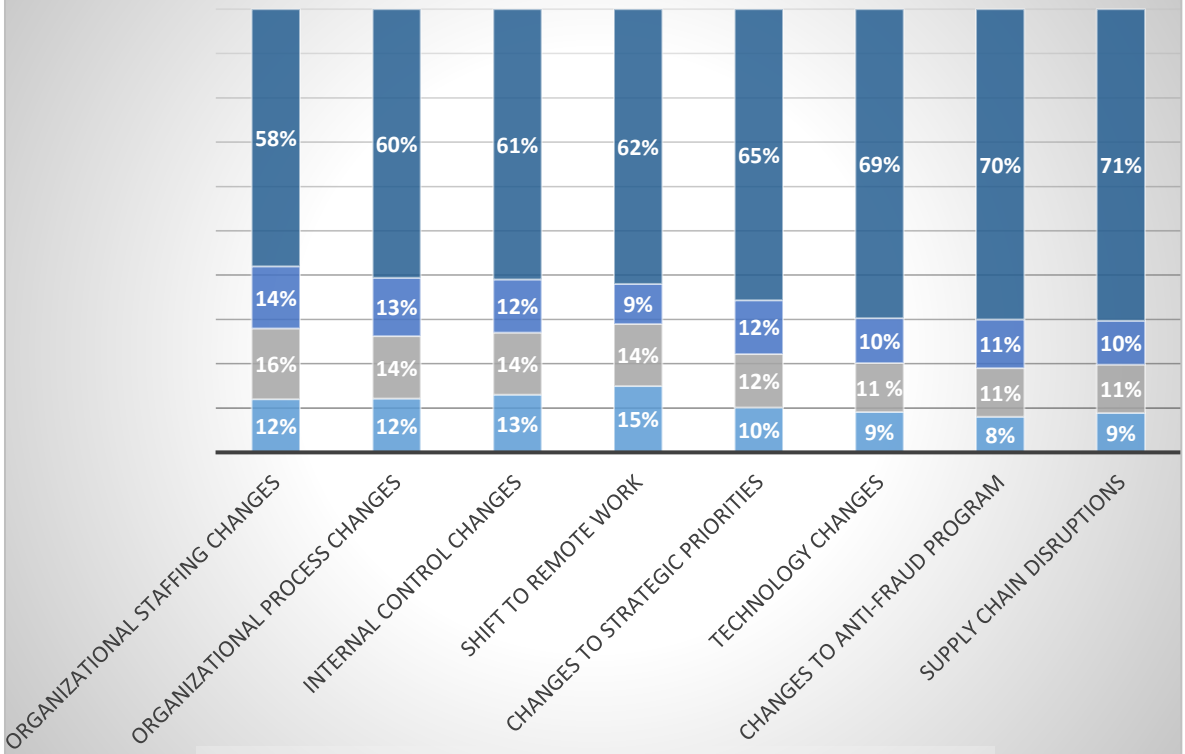
Die größten Fraudrisiken im Zusammenhang mit der Pandemie

Personalveränderungen und Telearbeit sind die größten Sorgen

Mehr als die Hälfte sieht, dass Faktoren der Pandemie zu Fraud beitragen

Bei der Erstellung ihres Berichts über beruflichen Fraud stellte die ACFE fest, dass 52 % der Befragten angaben, bei den von ihnen untersuchten Fraudfällen habe mindestens eines von mehreren pandemiebedingten Problemen zum Fraud beigetragen. Am häufigsten waren dabei pandemiebedingte personelle Veränderungen in der Organisation. Insgesamt 42 % der Befragten gaben an, dass Personalveränderungen signifikante, moderate oder geringfügige Faktoren seien, die zu beruflichem Fraud beitragen. Die Umstellung auf Telearbeit wurde am häufigsten als signifikanter Faktor genannt (15 %), gefolgt von internen Kontrollen (13 %) (siehe Abbildung 1).

Abbildung 1: Wie stark trugen Faktoren der Pandemie zu beruflichem Fraud bei?



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

Eine genauere Untersuchung einiger der wichtigsten im ACFE-Bericht identifizierten pandemiebedingten Probleme zeigt, dass die Auswirkungen oft komplex und subtil sein können.

Personalveränderungen bergen verschiedene Fraudrisiken

Die Pandemie zwang viele Organisationen dazu, Umgehungslösungen oder Abkürzungen zu finden, um die zahlreichen Störungen zu bewältigen. Dazu gehörten die Änderung oder Ausweitung der Aufgabenbereiche der Mitarbeiter oder die Einstellung neuer Mitarbeiter, die nur wenig Zeit hatten, sich in ihre Arbeit einzuarbeiten. Darüber hinaus wurden vorübergehende Entlassungen oder Beurlaubungen aufgrund der pandemiebedingten wirtschaftlichen Unsicherheit oft dauerhaft, bemerkte David Dominquez, Leiter für Revision und Compliance bei Itafos, einem Phosphat- und Spezialdüngemittelunternehmen. „Das hat das Risiko in vielerlei Hinsicht definitiv erhöht“, sagte er.

Angesichts der vielen Anpassungen und Anpassungen der Arbeitsabläufe und -protokolle, die die Pandemie möglicherweise mit sich gebracht hat – und der potenziellen Lernkurve für diejenigen, die neue Aufgaben übernehmen – sollten Organisationen überlegen, welche unbeabsichtigten Auswirkungen diese Änderungen möglicherweise hatten. Hier sind einige Bereiche, die berücksichtigt werden sollten:

Kultur

Es gibt viele Gründe, Unternehmenskultur und -werte nach der Pandemie zu überdenken und gegebenenfalls zu bekräftigen. „Es zum Laufen zu bringen“ war während der Pandemie eine Tugend, doch das kann bedeuten, dass wichtige ethische Praktiken und Einstellungen in Vergessenheit geraten sind. Neue Mitarbeiter haben möglicherweise auch nie eine angemessene Einführung in die ethischen Werte des Unternehmens erhalten. In diesem Fall sind Unternehmen gut beraten, ihre Mitarbeiter an die Erwartungen an ethisches Verhalten zu erinnern.

„Ein proaktiver Ansatz in Bezug auf die Unternehmenskultur kann verschiedene Arten von Fehlverhalten verhindern und Verhaltensweisen fördern, die die Arbeitsmoral und Produktivität steigern“, so die ACFE in ihrem Bericht. „Die Unternehmenskultur hat einen starken Einfluss darauf, wie Menschen ihre Arbeit erledigen, wie Entscheidungen über Qualität, Compliance und andere kritische Belange getroffen werden und wie die Organisation intern und extern wahrgenommen wird.“[14]

Überlegungen zum Personal

Ein Mangel an Arbeitskräften und veränderte Richtlinien für Hybrid- und Telearbeit haben einige langjährige Personalpraktiken, wie beispielsweise anonyme Whistleblower-Hotlines, auf den Kopf gestellt.

Ein wichtiges Instrument der Personalabteilung zur Fraudprävention ist die anonyme Whistleblower-Hotline. Laut dem ACFE-Bericht wurden 42 % der Fraudfälle durch Hinweise aufgedeckt – mehr als dreimal so viele wie bei der nächsthäufigsten Methode.

Die Interne Revision kann diesen Prozess unterstützen, indem sie prüft, ob er wie vorgesehen funktioniert. Der erste Schritt könnte darin bestehen, zu ermitteln, wie gut diese Hotlines überwacht werden und ob Beschwerden verfolgt werden, so Dominquez. Er empfiehlt, den Hotline-Zuständigen Fragen zu stellen wie:

- **Wie erreichen die Leute die Hotline?** Sie können Hinweise in einem Briefkasten im Büro hinterlassen, eine Hotline anrufen oder Beschwerden online melden. Bedenken Sie, dass ein Briefkasten – und Plakate, die für die Hotline werben – den Mitarbeitern im Homeoffice nicht helfen.
- **Kann die Hotline gegebenenfalls in verschiedenen Sprachen angeboten werden?**
- **Wie gut wird der damit verbundene Aufwand verfolgt?** Dominquez bemerkte, dass sich manche Unternehmen zu niedrigen Beschwerdezahlen gratulieren. Dies könnte ein gutes Zeichen für eine gut geführte Organisation sein, aber auch darauf hinweisen, dass manche Hotline-Anrufe nicht beantwortet oder Beschwerden nur selten verfolgt werden.

Die Interne Revision kann den Prozess der Beschwerdebearbeitung prüfen, um sicherzustellen, dass von der Beschwerdeaufnahme bis zur Beschwerdelösung ein angemessener Zeitrahmen eingehalten wird und dass die Entscheidungen zur Weiterverfolgung fundiert sind. Organisationen erhalten manchmal stichhaltige Hinweise auf Fraud nicht, weil nach einem Hinweis Vergeltungsmaßnahmen befürchtet werden. Die Interne Revision kann prüfen, ob das Unternehmenshandbuch oder der Verhaltenskodex Vergeltungsmaßnahmen ausdrücklich verbietet. Darüber hinaus kann die Interne Revision dem Unternehmen auch dabei helfen, herauszufinden, ob Hinweisgeber seltener befördert werden oder eher eine schlechte Leistungsbeurteilung erhalten, so Dominquez. Selbst wenn eine Beschwerde unbegründet ist, können Unternehmen im Laufe des Bearbeitungsprozesses Richtlinien finden, die aktualisiert oder präzisiert werden müssen, so Dominquez.

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

Zu den weiteren wertvollen Vorsichtsmaßnahmen/Kontrollen, die Organisationen fortsetzen oder umsetzen sollten, gehören:

- Hintergrundüberprüfungen zur Ermittlung früherer Kredit- oder anderer finanzieller Probleme oder einer Vorgeschichte von Lohnpfändungen, Pfandrechten oder Urteilen, die mit Unterschlagung in Verbindung stehen könnten.
- Überprüfung der Zertifizierungen.

Die ACFE berichtete, dass 50 % der Betrüger vor oder während des Fraudfalls mindestens ein Warnsignal im Personalbereich aufwiesen. Was das Verhalten betrifft, so war ein Leben über die eigenen Verhältnisse seit 2008 in jeder ACFE-Studie das am häufigsten festgestellte Warnsignal. Es wurde in 39 % der Fälle identifiziert und lag damit deutlich vor dem zweithäufigsten Faktor, finanziellen Schwierigkeiten, mit 25 %.

Arbeitsplatzunsicherheit

Die ACFE identifizierte eine Reihe von Beispielen für Arbeitsplatzunsicherheit, die zu Fraud beitragen kann. Schwierige wirtschaftliche Bedingungen können diese Unsicherheit noch verstärken. Zu den spezifischen Warnsignalen zählen:

- Angst vor dem Verlust des Arbeitsplatzes.
- Ablehnung von Gehaltserhöhung oder Beförderung.
- Kürzung der Sozialleistungen.
- Gehaltskürzung.
- Unfreiwillige Arbeitszeitverkürzung.
- Degradierung.

Obwohl sich das Wirtschaftsklima seit den schlimmsten Tagen der Pandemie stabilisiert hat, bleiben die Herausforderungen im globalen Geschäftsklima bestehen. Wenig überraschend blieben die Auswirkungen der Arbeitsplatzunsicherheit laut ACFE auch 2022 stark. Es liegt nahe, dass einige dieser Unsicherheiten weiterhin zu Fehlverhalten von Mitarbeitern führen können.

Diese Warnsignale gelten für Mitarbeiter im Allgemeinen, es gibt jedoch einige zusätzliche Warnsignale, die speziell für Führungskräfte in der Geschäftsleitung gelten:

- **Mobbing oder Einschüchterung.** 23 % für Eigentümer/Führungskräfte; 8 % für Nicht-Eigentümer/Führungskräfte.
- **Kontrollprobleme.** 18 % für Eigentümer/Führungskräfte; 12 % für Nichteigentümer/Führungskräfte.
- **„Wheeler-dealer"-Einstellung.** 17 % für Eigentümer/Führungskräfte; 9 % für Nichteigentümer/Führungskräfte.
- **Übermäßiger Druck innerhalb der Organisation.** 13 % für Eigentümer/Führungskräfte; 6 % für Nichteigentümer/Führungskräfte.
- **Frühere rechtliche Probleme.** 11 % für Eigentümer/Führungskräfte; 3 % für Nichteigentümer/Führungskräfte.

COVID-bedingte Änderungen bei internen Kontrollen sollten überprüft werden

Interne Kontrollen sind Verfahren, die sicherstellen, dass Maßnahmen und Entscheidungen innerhalb einer Organisationen Richtlinien, Berichtspflichten und Compliance-Vorgaben entsprechen. Fraudbekämpfungskontrollen können Fraudverluste reduzieren und die Aufdeckung von Fraudfällen beschleunigen. Laut der ACFE-Studie ließ sich fast die Hälfte der Fraudverluste auf zwei Faktoren zurückführen: fehlende interne Kontrollen (29 %) und die Außerkraftsetzung bestehender Kontrollen (20 %). Implementierung und Stärkung interner Kontrollen können Organisationen deutliche Vorteile bringen. Die Interne Revision spielt eine wichtige Rolle bei der Berichterstattung über interne Kontrollen und der Empfehlung von Verbesserungsvorschlägen. Tatsächlich ergab die ACFE-Umfrage, dass der durchschnittliche Fraudverlust um 50 % höher war (150.000 USD gegenüber 100.000 USD), wenn keine Interne Revision vorhanden war.

Interne Revisoren, die an der IAF/Kroll-Umfrage teilnahmen, waren der Ansicht, dass „der interne Kontrollrahmen aufgrund der Herausforderungen der Telearbeit und in vielen Fällen aufgrund von Personalkürzungen durch Krankheit, Kurzarbeit und Personalabbau geschwächt wurde“.[15]

Neue Mitarbeiter, die in Krisenzeiten in Organisationen eintreten, haben möglicherweise nicht ausreichende Schulungen erhalten oder es mangelt ihnen an Wissen, oder sie haben nur Notfallprotokolle gelernt, die langjährige Prozesse und Kontrollen nicht berücksichtigen, so Dominquez. „Kontrollen wurden verwässert oder sind vielleicht einfach durch die Maschen gefallen“, sagte er. Solche Abkürzungen können sich im Laufe der Zeit als Standardverfahren etablieren – und bleiben es auch, obwohl sie eigentlich nur für einen bestimmten Zeitraum oder eine bestimmte Situation gedacht waren.

Diese Sorge hat in vielen Organisationen zu positiven Veränderungen geführt. So gaben etwa drei Viertel der Mitglieder des Prüfungsausschusses in einer gemeinsamen Umfrage des Deloitte Center for Board Effectiveness und des Center for Audit Quality an, dass sie ihre internen Kontrollen im letzten Jahr aufgrund der Telearbeitsumgebung aktualisiert hätten.[16]

Schwachstellen in den internen Kontrollen können zu Fraud beitragen, indem sie ein Umfeld schaffen oder fördern, in dem wirksame Fraudbekämpfungsmaßnahmen leichter vernachlässigt oder außer Kraft gesetzt werden können. Beispielsweise wurde während der Pandemie möglicherweise die Funktionstrennung – eine gängige und wirksame Maßnahme zur Fraudbekämpfung – außer Kraft gesetzt, weil sie aufgrund der Verstreuung der Mitarbeiter über verschiedene Standorte oder aufgrund von Personalabbau oder -engpässen schwieriger umzusetzen war. Unternehmen sollten diese Art der internen Kontrolle jetzt überprüfen, um sicherzustellen, dass sie wiederhergestellt wurde und effektiv funktioniert.

Die Interne Revision kann Organisationen dabei unterstützen, diese Risiken zu adressieren, indem sie die Einhaltung wichtiger Protokolle und Prozesse sicherstellt. Mithilfe von Process-Mapping-Technologie kann sie Prozesse über einen Zeitraum von sechs Monaten oder einem Jahr hinweg verfolgen und Abweichungen von den geltenden Richtlinien oder Best Practices identifizieren. „Sie erkennt Abweichungen von Standardverfahren oder -richtlinien und kann feststellen, welche Prozesse aktualisiert oder durchgesetzt werden müssen“, so Dominquez.

Zu den weiteren Bereichen, die erneut überprüft werden müssen, gehören interne Kontrollen im Zusammenhang mit Beschaffung, Scheckausstellung, Bankabstimmungen, Spesenrückerstattungen oder allen Bereichen, die mit finanziellen Überlegungen verbunden sind.

Telearbeit bleibt kritischer Fraudfaktor

Die drastische Umstellung auf Telearbeit – die Schließung von Büros und die Möglichkeit für Mitarbeiter, ihre Arbeit von zu Hause zu erledigen – war für die meisten Organisationen während der Pandemie wahrscheinlich die bedeutendste Veränderung. Folglich wurde dieser neue Ansatz im ACFE-Bericht am häufigsten als Faktor genannt, der maßgeblich zu Fraud beiträgt. Unter normalen Umständen würde ein Unternehmen die strategischen Auswirkungen einer solchen Umstellung monatelang abwägen, doch angesichts der Unsicherheit und Dringlichkeit der ersten Wochen der Pandemie war dies praktisch unmöglich. Wenn man allein und außer Sichtweite von Kollegen und Vorgesetzten arbeitet, kann dies zumindest verschiedene Fraudfälle erleichtern. Wer dauerhaft auf Tele- oder Hybridarbeit umstellt oder umgestiegen ist, sollte laut ACFE einen Change-Management-Plan durchführen, „um die Schwachstellen zu erkennen, die katastrophale Folgen haben können, wenn sie nicht behoben werden“.[17]

Im Laufe dieses Prozesses ergeben sich mehrere potenzielle Schwachstellen, auf die sich die Interne Revision konzentrieren könnte. So wurden laut dem IAF/Kroll-Bericht beispielsweise die Schwierigkeiten der effektiven Personalführung in einer fragmentierten Remote-Umgebung und deren Auswirkungen auf die Unternehmenskultur als zentrale Bereiche genannt.[18] Ethisches Verhalten wird oft durch den Umgang mit anderen Mitarbeitern erlernt und gefestigt, die es im Job vorleben. Der Kontakt zu erfahreneren Kollegen kann Mitarbeitern helfen, in verwirrenden oder verdächtigen Situationen zu reagieren, beispielsweise wenn ein anderer Mitarbeiter sich unangemessen oder illegal verhält.

Zu den Fraudarten, die speziell mit der Telearbeit in Verbindung gebracht werden, gehören:

[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.

- **Arbeitszeitdiebstahl oder ungenaue Angaben zu den geleisteten Arbeitsstunden.** Dies kann einfacher sein, wenn jemand nicht direkt beaufsichtigt wird.
- **Datendiebstahl oder -missbrauch oder Weitergabe vertraulicher oder sensibler Informationen.** Dies kann geschehen, wenn Personen Zugriff auf die Geräte eines Mitarbeiters haben, oder wenn Mitarbeiter sich beim Datenmissbrauch außerhalb des Büros wohler fühlen.[19]

Ein damit verbundenes Problem sind Nebenjobs von Remote-Mitarbeitern. So kann ein Mitarbeiter beispielsweise während seiner Arbeitszeit für seinen Hauptarbeitgeber Beratungs- oder Zeitarbeitsaufträge für ein anderes Unternehmen übernehmen, so Dominquez. Dies ist sicherlich Arbeitszeitdiebstahl, doch der Missbrauch von Unternehmensressourcen wie Laptops oder Telefonen kann das Unternehmen auch Cybersicherheitsproblemen aussetzen. Die Nebentätigkeit kann zudem einen Interessenkonflikt darstellen, wenn der Mitarbeiter für einen Konkurrenten arbeitet, insbesondere wenn er Informationen weitergibt, die für die Konkurrenz von Nutzen sind. Die Interne Revision kann helfen, dieses Problem zu lösen, indem sie die Art der Mitarbeiterschulung hinterfragt und prüft, ob das Mitarbeiterhandbuch und die Richtlinien an neue Arbeitsumgebungen angepasst wurden, so Dominquez.

Technologische Veränderungen führen zu Geben und Nehmen bei Fraud

Technologie kann Organisationen dabei helfen, wirksame Verfahren in Bereichen wie interner Kontrolle und Telearbeit zu implementieren. Unternehmen haben bereits Verbesserungen und Investitionen in Technologie vorgenommen, um Cybersicherheitsbedenken zu begegnen, und die Pandemie hat die Unternehmen dazu bewogen, ihre Systeme zu beschleunigen und zu stärken. Viele Interne Revisionen wurden in die Technologie-Upgrades einbezogen. Tatsächlich haben 29 % der Internen Revisoren seit Beginn der Pandemie Datenanalysen zu ihren Instrumenten zur Aufdeckung von Fraud und Korruption hinzugefügt.[20]

Gleichzeitig kann der Missbrauch oder die Vernachlässigung von Technologie-Tools Fraudversuchen den Erfolg erleichtern. Wie bereits erwähnt, ist Datendiebstahl eine der Gefahren im Zusammenhang mit Telearbeit. Mögliche Lösungen gegen Datendiebstahlrisiken sind laut ACFE beispielsweise die Verpflichtung der Mitarbeiter, ihr Heimnetzwerk zu sichern und es nicht mit anderen Familienmitgliedern zu teilen. Die Verwendung von VPNs sowie stärkeren und komplexeren Passwörtern und Einstellungen zur Sicherung von Heimcomputern ist ebenfalls wichtig. Weitere Optionen sind Multi-Faktor-Authentifizierung und jährliche Schulungen für Mitarbeiter zum Thema Datensicherheit und Datenschutz. Unternehmen sollten außerdem Richtlinien für die akzeptable Nutzung elektronischer Geräte, sozialer Medien und Unternehmensdaten entwickeln und von den Mitarbeitern verlangen, diese zu lesen und deren Kenntnisnahme zu bestätigen.

Organisationen, die eine Telearbeits- oder Hybridumgebung nutzen, müssen außerdem sicherstellen, dass ihre Mitarbeiter Software und Sicherheitspatches auf ihren Heimgeräten aktualisieren und sie über die besten Möglichkeiten zur Vermeidung von Phishing und anderen Hackerbedrohungen aufklären.[21] Unternehmen, die sich mit den Auswirkungen der Pandemie auseinandersetzen mussten, sollten natürlich ihre eigenen Cybersicherheitsmaßnahmen überprüfen, um sicherzustellen, dass sie auf dem neuesten Stand bleiben.

Um diese Bedenken auszuräumen, empfahl Dominquez, dass die Interne Revision untersuchen sollte, welche Sicherheitsprotokolle vorhanden sind, welche Tools zur Verhinderung von Datenverlusten das Unternehmen verwendet werden, ob Multi-Faktor-Authentifizierung und VPNs erforderlich sind, und ob Konten rechtzeitig deaktiviert werden, wenn Mitarbeiter das Unternehmen verlassen.

„Quiet Quitting“ beeinträchtigt Compliance und Ethikbemühungen

Unter „Quiet Quitting“ versteht man die Praxis, dass Arbeitnehmer nur das absolute Minimum ihrer Arbeit erledigen. Einer Schätzung von Gallup zufolge machen solche Arbeitnehmer mindestens 50 % der US-amerikanischen Erwerbsbevölkerung aus. Der Anteil der engagierten Arbeitnehmer lag bei 32 %, der der aktiv desinteressierten Arbeitnehmer jedoch bei 18 %. Gallup weist darauf hin, dass dies in einer Zeit, in der viele Arbeitsplätze kollaborativ sind oder zur Erfüllung von Kundenanforderungen möglicherweise zusätzliche Schritte erforderlich sind, besonders problematisch ist. Und obwohl der Trend zum Quie Quitting viel Aufmerksamkeit erregt hat, sollten sich Arbeitgeber darüber im Klaren sein, dass es immer noch lautstarke Quittierer gibt – also Menschen, die ihre Unzufriedenheit aktiv ausdrücken und vielleicht sogar verbreiten.[22]

[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.
[22] “Is Quiet Quitting Real?” Jim Harter, Gallup Workplace, September 6, 2022.

Dieser Trend kann sich negativ auf Produktivität, Effizienz und Mitarbeiterbindung auswirken. Gleichzeitig kann er sich negativ auf das Risikomanagement auswirken. „Die Mitarbeiter achten nicht mehr so genau darauf, was sie tun sollten“, so Dominquez. Und wie *Corporate Compliance Insights* anmerkt, erfordert ein erfolgreiches Compliance- und Ethikprogramm die Beteiligung und Unterstützung aller Mitarbeiter eines Unternehmens. „Kombiniert man eine relativ negative Arbeitseinstellung mit einem Ansatz, der auf minimalen Arbeitsergebnissen basiert, fehlen oft die zusätzlichen Maßnahmen, auf die Compliance- und Ethikexperten angewiesen sind, um sicherzustellen, dass Mitarbeiter Probleme ansprechen“, heißt es in der Stellungnahme.[23]

Dies gilt sicherlich auch für ein Fraudrisikomanagementprogramm. Mitarbeiter könnten Genehmigungen und Transaktionen einfach absegnen oder Anomalien ignorieren. Oder sie können eine Anomalie eskalieren lassen, nur um dann festzustellen, dass ihr Vorgesetzter auf der nächsten Ebene sie ignoriert, weil sie stillschweigend kündigen.

Die Interne Revision kann Mitarbeiterzufriedenheitsumfragen, Fluktuationsraten und Austrittsgespräche untersuchen, um ein Gefühl für Probleme beim Mitarbeiterengagement zu bekommen. Aktuelle Trends können mit der Entwicklung vor der Pandemie verglichen werden, um zu verstehen, welche Auswirkungen sie möglicherweise hatte, sagte Dominquez.

[23] “Why ‘Quiet Quitting’ Could Harm Ethics and Compliance Functions,” Lisa Beth Lentini Walker, Corporate Compliance Insights, September 14, 2022.

Fazit

Was bedeutet das alles? Laut ACFE verlieren Unternehmen jährlich schätzungsweise 5 % ihres Umsatzes durch Fraud. Der Median des Verlusts beträgt 117.000 US-Dollar, der durchschnittliche Verlust 1.783.000 US-Dollar. Durchschnittlich können die Verluste durch Fraudmethoden 8.300 US-Dollar pro Monat betragen. Das sind für jedes Unternehmen ernstzunehmende Faktoren.

Während und seit dem Höhepunkt der Pandemie haben sich Unternehmen an Interne Revisoren gewandt, um strategische Entscheidungsträger bei der Neubeurteilung und Verbesserung ihrer Betriebsprozesse zu unterstützen. Diese Praxis sollte fortgesetzt werden, insbesondere bei der Bewertung interner Kontrollen zur Fraudbekämpfung. Die Welt mag die Pandemie überwunden haben, aber die pandemiebedingten Fraudgefahren sind nicht unbedingt verschwunden.

Seit Beginn der Pandemie wird der Beitrag der Internen Revision zur Eindämmung oder Verhinderung von Fraud noch stärker geschätzt. Früher wurde die interne Revision oft erst eingeschaltet, wenn bereits ein Fraudfall eingetreten war. Dies ändert sich nun. Organisationen warten heute weniger darauf, Fraud zu erkennen, sondern bekämpfen Fraud, bevor zu großer Schaden entsteht. Um dies zu erreichen, werden Interne Revisoren in präventive Gespräche eingebunden, d. h. sie werden aufgefordert, über Maßnahmen zur Fraudbekämpfung nachzudenken, bevor es zu Fraud kommt, so Dominquez. Die Interne Revision fördert außerdem Diskussionen über die Beurteilung von Fraudrisiken und Fraudrisiko-Rahmenwerke, wobei sie die Häufigkeit und Wirksamkeit dieser Beurteilungen und Kontrolltests berücksichtigt und alle Änderungen im laufenden Risikoprofil des Unternehmens erfasst. „Anstatt abzuwarten, bis Fraud erkannt wird, gehen Interne Revisoren präventiv vor“, so Dominquez.

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

Deutsche Übersetzung durch DIIR – Deutsches Institut für Interne Revision e.V., September 2025

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