ACAMS ENTERPRISE

Best-Practice-Leitfaden:

Betrugsrisikoanalyse

Inhalt

1. Einführung **3**

2. Die aktuelle Situation der Betrugsrisikoanalyse **4**

2.1 Arten der Betrugsrisikoanalyse und aktueller Stand 4

2.2 Business Case erstellen 5

3. Eine umfassende Methodik **7**

3.1 Ein schrittweiser Ansatz zur Betrugsrisikoanalyse 7

3.2 Ergebnisse überprüfen und präsentieren 10

3.3 Maßnahmenplan und Kontrollpunkte 10

4. Den Status quo verbessern **11**

4.1 Analysieren, wo Sie gerade stehen 11

4.2 Sinnvolle Verbesserungen identifizieren 11

5. Die Zukunft der Betrugsrisikoanalyse **12**

5.1 Live-Dashboards 12

5.2 Silos aufbrechen 13

6. Fazit **14**

7. Anhang A: Betrugstaxonomie **15**

8. Anhang B: Risikopriorisierungsmatrix **16**

9. Anhang C: Betrugsrisikoregister **17**

10. Anhang D: Beispiel für ein Dashboard zur Betrugsrisikoanalyse **20**

1. Einführung

ACAMS hatte sich zum Ziel gesetzt, Best Practices für die Durchführung von Betrugsrisikoanalysen zu finden, und führte mehrere Round Table-Gespräche und Interviews mit Fachleuten von Banken und Finanzdienstleistern durch.

Die Branche verfolgt bei der Betrugsrisikoanalyse keinen einheitlichen Ansatz. Die Bandbreite der Organisationen reicht von Unternehmen, die nie eine Betrugsrisikoanalyse durchführen, bis hin zu solchen, die diese lediglich als reine Pflichtübung betrachten. Reifere Unternehmen haben die Betrugsrisikoanalyse in ihren unternehmensweiten Risikoanalyseprozess integriert.

Führungskräfte im Bereich Betrugsbekämpfung waren unterschiedlicher Ansicht. Viele betrachteten die Betrugsrisikoanalyse als administrative Maßnahme, die ihnen nur das bestätigte, was sie bereits wussten. Dennoch haben sich einzelne Best-Practice-Beispiele herausgebildet, bei denen Unternehmen – entweder zur Verlustminimierung oder als Reaktion auf regulatorischen Druck – umfassendere und ganzheitlichere Betrugsrisikoanalysen durchführen.

In diesem Best-Practice-Leitfaden untersuchen wir, wie Daten erfasst, Betrugsrisikoanalysen durchgeführt und Ergebnisse analysiert werden, um wichtige Risikobereiche für Investitionen zu priorisieren. Bei effektiver Nutzung kann die Risikoanalyse die effektivste und beste Verteidigung gegen Betrug sein.

2. Die aktuelle Situation der Betrugsrisikoanalyse

2.1 Arten der Betrugsrisikoanalyse und aktueller Stand

Unser Ziel war es, zu verstehen, wie Unternehmen das Betrugsrisiko für Kunden und ihr Geschäft bewerten. Nachfolgend sind die wichtigsten Prozesse zusammengefasst, mit denen Unternehmen das Betrugsrisiko bewerten:

2.1.1. Die Kundenrisikobewertung (Customer Risk Assessment – CRA) legt den Schwerpunkt auf AML und wird in erster Linie dort eingesetzt, wo regulatorische Vorschriften zur Risikobewertung in Bezug auf Kunden bestehen. Die Kundenrisikobewertung bewertet das Risiko, dass der Kunde Betrug begeht, wie beispielsweise First-Party-Betrug oder Antragsbetrug. Häufig stehen First-Party-Betrug und Antragsbetrug im Zusammenhang mit Kreditverfahren. Unternehmen können die Grundsätze zur Bewertung dieser Betrugsarten jedoch auf die meisten Finanzprodukte anwenden.

2.1.2. Die Produktrisikobewertung umfasst die Beurteilung des mit einem Finanzprodukt verbundenen Risikos unter Berücksichtigung von Faktoren wie dem Vertriebskanal und den beteiligten Ländern. Beispielsweise stellen grenzüberschreitende Überweisungen ein höheres Risiko dar, da historische Daten zeigen, dass die meisten betrügerischen Transaktionen grenzüberschreitend sind.[1]. Führungskräfte im Bereich Betrugsbekämpfung verwiesen auf agile Arbeitsmethoden in Änderungsprojekten, bei denen Betrugskontrollen Teil der abschließenden User Stories sind. Wenn ein Produkt- oder Entwicklungsteam Betrugskontrollen nicht in die ursprüngliche Produktkonzeption einbezieht, sondern erst später durchführt, besteht eine zusätzliche Betrugsgefährdung.

2.1.3. Die unternehmensweite Risikoanalyse ist die Praxis der Bewertung von Risiken für das Unternehmen. Dazu gehört die Identifizierung verschiedener Risikoarten und die Implementierung von Prozessen, die Risikokontrollen abbilden. Anschließend werden die Risikokontrollen auf ihre Effektivität überprüft und die Residualrisiken berechnet. Das Unternehmen kann dann die Residualrisiken anhand ihrer Wahrscheinlichkeit und Auswirkung priorisieren. Dadurch kann das Unternehmen angemessen investieren und Ressourcen für die Betrugsrisikoanalyse richtig zuweisen. Die regulatorischen Verpflichtungen von AML-Teams zur Durchführung von Risikoanalysen variieren je nach Land.

In diesem Best-Practice-Leitfaden konzentrieren wir uns darauf, wie man unter Berücksichtigung der externen und internen Betrugsrisiken eine Betrugsrisikoanalyse durchführt. Wir möchten Unternehmen auf die zukünftige Betrugslandschaft vorbereiten, indem wir eine Kombination aus historischen, aktuellen und szenariobasierten Zukunftstrends präsentieren.

1. Bericht über Betrug im Zahlungsverkehr 2024, gemeinsam veröffentlicht von der Europäischen Bankenaufsichtsbehörde und der Europäischen Zentralbank. https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud

2.2 Business Case erstellen

Die COVID-19-Pandemie hat gezeigt, dass Kriminelle ihre Angriffe auf Unternehmen und Institute konzentrieren, die entweder direkten Zugang zu Geld oder zu Produkten oder Dienstleistungen mit leicht übertragbarem Geldwert haben. Finanzinstitute, darunter sowohl Banken als auch Nichtbanken, sind daher besonders gefährdet.

Die Durchführung einer umfassenden Betrugsrisikoanalyse erfordert jedoch sorgfältige Planung, Ressourcen und Managementkapazitäten. Daher müssen Sie möglicherweise einen überzeugenden Business Case vorlegen, um diese Maßnahme in Ihrem Unternehmen umzusetzen.

Verluste durch Betrug haben zwangsläufig finanzielle Auswirkungen auf ein Unternehmen, können aber auch in anderer Hinsicht enorme negative Folgen haben:

- Vertrauensverlust von Anteilseignern und anderen Stakeholdern
- Verstärkte Kontrollen durch Strafverfolgungs- und Regulierungsbehörden mit potenziellen Geldstrafen oder strafrechtlichen Maßnahmen gegen Schlüsselpersonen
- Interner Vertrauensverlust in das Managementteam, was zu einer erhöhten Fluktuation bei Mitarbeitern und Führungskräften führen kann
- Sonstige Kosten, wie z. B. Rechtskosten und höhere Versicherungsprämien
- Reputationsschaden in den Medien und bei Kunden, was zu einem weiteren Vertrauensverlust nicht nur in das Unternehmen, sondern auch in das Finanzsystem führt
- Verlust des Wettbewerbsvorteils

Der Reputationsschaden kann im Großkundengeschäft größer sein als im Privatkundengeschäft. Der Grund dafür ist, dass Betrugsangriffe auf eine Großhandelsbank in Bezug auf Volumen und Wert wahrscheinlich viel höher sind als auf eine Privatkundenbank.

Letztendlich hilft eine solide Betrugsrisikoanalyse einem Unternehmen:

- effektive, risikobasierte Entscheidungen hinsichtlich Betrugskontrollen zu treffen, sodass die Maßnahmen und Ressourcen priorisiert werden können
- eine Investitionsanalyse für die Budgetausgaben durchzuführen
- eine stabile und umfassende Grundlage zu schaffen, auf die das Unternehmen zurückgreifen kann, wenn neue Betrugsarten und Bedrohungen auftreten oder Produkte und Dienstleistungen geändert werden
- Verluste durch Betrug zu mindern und andere damit verbundene Kosten wie Betriebs-, Verwaltungs- und Untersuchungskosten zu reduzieren

Die regelmäßige Durchführung von Betrugsrisikoanalysen ist besonders dringlich, da Finanzinstitute weltweit zunehmend Kunden für Verluste durch sogenannte „Authorized Push Payment“ (APP)-Betrugsfälle entschädigen. Im Vereinigten Königreich sind Banken gesetzlich verpflichtet, Verluste durch APP-Betrug zu erstatten. Andere Länder erwägen ähnliche Vorschriften. Viele renommierte Finanzinstitute erstatten freiwillig die Kosten für APP-Betrug, um das Vertrauen und die Loyalität ihrer Kunden aufrechtzuerhalten.

Laut der Financial Times ergab eine Umfrage unter 28.000 Personen, dass vierzig Prozent der Betrugsopfer im Vereinigten Königreich, 32 % in den USA und 14 % in Japan von ihrer Bank vollständig entschädigt wurden.[2]

Die Reduzierung von betrugsbedingten Verlusten und die Wahrung des guten Rufs und des Kundenvertrauens sind die Hauptgründe für die Notwendigkeit einer Betrugsrisikoanalyse. Ohne einen ganzheitlichen Ansatz ist die Risikominderung bestenfalls ein sporadisches Unterfangen und schlimmstenfalls reine Zeitverschwendung, wenn die größten Risiken nicht angegangen werden.

2. Britische Banken zahlen im Betrugsfall eher Entschädigungen als ihre ausländischen Konkurrenten, Financial Times, 28. September 2024 https://www.ft.com/content/bbe888ac-8888-40f6-9fb5-d89150025d36

3. Eine umfassende Methodik

3.1 Ein schrittweiser Ansatz zur Betrugsrisikoanalyse

Wie in der folgenden Abbildung zusammengefasst, lässt sich eine Betrugsrisikoanalyse in vier wesentliche Phasen unterteilen: Risikoidentifizierung, Risiko- und Kontrollanalyse, Residualrisikobewertung und Risikobehandlung.

Abbildung 1: Betrugsrisikoanalyse – Phasen

Die folgende Tabelle enthält eine detaillierte Aufschlüsselung der Phasen des Betrugsrisikomanagements mit einer Beschreibung der einzelnen Schritte. Bei der Risikoidentifizierung wird untersucht, wie Kriminelle Geschäftsprozesse ausnutzen können, während die Risiko- und Kontrollanalyse die Effektivität der aktuellen Kontrollen gegenüber identifizierten Risiken bewertet. Die Residualrisikobewertung befasst sich dann mit den Risiken, die nach Anwendung der Kontrollen verbleiben, und vergleicht sie mit den Toleranzwerten des Unternehmens. Schließlich konzentriert sich die Risikobehandlung auf Strategien zur Reduzierung der Residualrisiken auf ein akzeptables Niveau und fördert einen ausgewogenen und proaktiven Ansatz zur Betrugsprävention.

Risikoidentifizierung

Schritt 1: Eine Betrugstaxonomie erstellen

Eine Betrugstaxonomie dokumentiert alle historischen, aktuellen und potenziellen zukünftigen Betrugsszenarien, die sich auf Ihr Unternehmen auswirken könnten, wobei der Schwerpunkt auf relevanten Betrugsrisiken liegt:

Historische Trends: Frühere Betrugsfälle, von denen Ihr Unternehmen betroffen war.

Branchentrends: Betrugsarten, die weltweit von ähnlichen Unternehmen beobachtet wurden und auch Sie betreffen könnten.

Regionale Trends: Betrugsarten, die andere Sektoren in Ihrer Region betreffen, wie beispielsweise Geldwäsche, die auf Studierende im Vereinigten Königreich abzielt, oder Betrugsmaschen, die auf Arbeiter in den Vereinigten Arabischen Emiraten abzielen.

Szenarioplanung: Potenzielle zukünftige Betrugsfälle, wie beispielsweise Identitätsdiebstahl mithilfe künstlicher Intelligenz.

Eine Taxonomie bietet eine gemeinsame Sprache zur Beschreibung und Erfassung von Betrugsfällen.

Anhang A enthält ein Beispiel für die Erstellung einer Taxonomie.

Schritt 2: Relevante Mitarbeiter durch eine Umfrage einbinden

Alle Mitarbeiter, die mit Betrug und Betrugskontrollen befasst sind, in die Durchführung der Risikoanalyse einzubinden, gewährleistet das bestmögliche Ergebnis. Wenn Sie mit einer Umfrage oder einem Fragebogen beginnen, werden die folgenden Best Practices empfohlen:

- Beziehen Sie die Teilnehmer frühzeitig ein und erklären Sie ihnen den Zweck und die Bedeutung, damit dies nicht als Zeitverschwendung angesehen wird.
- Halten Sie die Stakeholder über den Prozess und die Ergebnisse auf dem Laufenden. Beziehen Sie Mitarbeiter mit Kundenkontakt wie Callcenter-Mitarbeiter, Filialmitarbeiter, Vermittler und Kundenbetreuer ein.
- Verwenden Sie offene Fragen, um Erkenntnisse zu gewinnen, die Ihnen sonst möglicherweise entgehen würden.

Schritt 3: Umfragedaten mit bekannten Betrugsfällen abgleichen

Die vorhandenen Betrugsdaten, KPIs, KRIs und Schadensfallkennzahlen müssen mit den Umfrageergebnissen zusammengeführt werden. Fokusgruppen und Interviews können dabei helfen, Unterschiede in den Datenpunkten auszugleichen und ein tieferes Verständnis der Umfrageergebnisse zu gewinnen.

Schritt 4: Interviews durchführen und die Ergebnisse überprüfen

Eine gründliche Erstbewertung liefert eine solide Ausgangsbasis, sodass sich künftige Überprüfungen auf geschäftliche Veränderungen und neu auftretende Betrugsrisiken konzentrieren können. Die Umfrage kann durch Maßnahmen zur Identifizierung weiterer Risiken und Schwachstellen ergänzt werden, wie z. B.:

- Befragung von Führungskräften, die Funktionen mit inhärenten Betrugsrisiken beaufsichtigen.
- Unabhängige Bewertung wichtiger Prozesse durch Dokumentenprüfungen und Interviews.
- Moderation von Workshops mit Mitarbeitern der zu bewertenden Geschäftsbereiche.
- Abhalten von Workshops mit Betrugsexperten, um ein Brainstorming zukünftiger Betrugsmaschen durchzuführen.
- Überprüfung von Betrugsinformationen, früheren Risikobewertungen, Untersuchungen oder Fallstudien aus anderen Branchen.

Risiko- und Kontrollanalyse

Schritt 1: Eine Risiko-analysematrix verwenden

Die Betrugsrisikoanalyse umfasst die Abschätzung der Wahrscheinlichkeit und der Folgen jedes Risikos unter Verwendung einer Risikopriorisierungsmatrix, um Risiken anhand dieser Faktoren zu bewerten (siehe Anhang B).

- **Eintrittswahrscheinlichkeit:** Bewertet die Wahrscheinlichkeit und Häufigkeit von Betrugsfällen unter Berücksichtigung von Faktoren wie Transaktionsvolumen, Nutzen für den Betrüger und frühere Betrugsfälle
- **Schadenshöhe:** Bewertet die Dauer (Zeit bis zur Aufdeckung des Betrugs) und die Auswirkungen (Schweregrad). Die Folgen können finanzielle Verluste, Verlust von Dienstleistungen, Probleme mit der Kundenzufriedenheit, operative Belastungen, sinkende Mitarbeitermoral, Reputationsschäden und Schaden für die Opfer sein.

Eine Risikopriorisierungsmatrix oder Heatmap hilft dabei, den Zusammenhang zwischen der Wahrscheinlichkeit eines Risikos und der Schwere seiner Auswirkungen zu visualisieren.

Schritt 2: Wichtige Kontrollen identifizieren

Nach der Identifizierung und Priorisierung der Risiken werden Kontrollen zugewiesen und bewertet, indem folgende Fragen gestellt werden:

- Welche Kontrollen gibt es für jedes Risiko?
- Sind sie korrekt implementiert und funktionieren sie wie vorgesehen?
- Reichen sie aus, um das identifizierte Betrugsrisiko zu mindern?

Schritt 3: Effektivität der Kontrollen bestätigen

Die Ergebnisse der Gespräche mit Geschäftsinhabern sollten:

- die Ergebnisse der Prüfungen unterstützen bzw. ergänzen
- Überwachungshandlungen verwenden, um die Effektivität der Kontrollen (Konzeption und operative Effektivität) zu überprüfen
- zur Bestätigung auf alle vorhandenen Selbsteinschätzungen zu Risiken und Kontrolleffektivität verweisen

Schritt 4: Bewertungen gemeinsam mit Geschäftsverantwortlichen bestätigen

An dieser Stelle ist es sinnvoll:

- die Risikopriorisierungsmatrix gemeinsam mit den Geschäfts- und Prozessverantwortlichen zu überprüfen
- die Kontrollbewertungen zu bestätigen, bevor Sie mit dem nächsten Schritt fortfahren

Residualrisikobewertung

Schritt 1: Risiken anhand der Risikobereitschaft und -toleranz des Unternehmens bewerten

- Überprüfen Sie die Risikobereitschaft und -toleranz des Unternehmens, wie in ihrer Risikomanagementrichtlinie definiert.
- Bewerten Sie Betrugsrisiken anhand dieser vordefinierten Niveaus.
- Berücksichtigen Sie die Art des Unternehmens, um dessen spezifische Betrugsrisikotoleranz zu bestimmen.

Schritt 2: Weitere Maßnahmen erwägen

Für Risiken, die über der Toleranzschwelle liegen, sollten Sie verschiedene Optionen in Betracht ziehen:

- Das Risiko vermeiden, indem die risikobehaftete Aktivität eingestellt wird
- Risiken innerhalb der Toleranzgrenzen akzeptieren, indem die bestehenden Kontroll- und Überwachungshandlungen beibehalten werden
- Weitere Analysen mit einem Audit oder einem Kontroll-„Stresstest" durchführen
- Kontrollen hinzufügen, um die Wahrscheinlichkeit oder die Auswirkungen des Risikos zu verringern

Schritt 3: Kosten und Nutzen abwägen

Wägen Sie den Nutzen neuer Kontrollen gegen deren Kosten und Umsetzungsaufwand ab.

Akzeptieren Sie ein Risiko außerhalb der Toleranzgrenzen, wenn:

- der Nutzen der Aktivität die Risikofolgen überwiegt
- zusätzliche Risikomitigierungskosten oder Zeitpläne sich negativ auf wesentliche Aktivitäten auswirken

Ergreifen Sie folgende Maßnahmen:

- Beziehen Sie erfahrene Geschäftsverantwortliche ein, um Betrugsbekämpfungsmaßnahmen im Hinblick auf die Risikotoleranz zu bewerten.
- Verwenden Sie eine Tabelle für Risikomanagementmaßnahmen (siehe Anhang B), um Maßnahmen basierend auf dem Betrugsrisikoniveau zu ergreifen.

Risikobehandlung

Schritt 1: Risikobehandlungsoptionen in Betracht ziehen

Zu den Optionen gehören:

- Aufrechterhaltung bestehender Kontrollen
- Verbesserung der aktuellen Kontrollen
- Entwicklung neuer Kontrollen und Aktualisierung von Prozessen (siehe Beispiel in Anhang C2)

Kontrollen lassen sich in drei Kategorien einteilen:

- **Aufdeckung:** Betrug identifizieren, sobald er stattfindet
- **Prävention:** Betrug verhindern, bevor er passiert (z. B. durch Cybersicherheitsprotokolle, die unbekannte Logins sperren)
- **Reaktion:** Maßnahmen ergreifen, nachdem ein Betrug stattgefunden hat (z. B. Sperrung zukünftiger Kartentransaktionen)

Schritt 2: Wahrscheinlichkeit oder Folgen ermitteln

- Die meisten Kontrollen zielen darauf ab, die Wahrscheinlichkeit von Betrug zu verringern.
- Einige Kontrollen zielen darauf ab, die Folgen von Betrug zu verringern.

Beispiel: Die Senkung der täglichen Abhebungslimits an Geldautomaten kann finanzielle Verluste reduzieren, wenn ein Betrüger die vorbeugenden Kontrollen umgeht.

Schritt 3: Residualrisiken bewerten und priorisieren

- Bewerten Sie die Auswirkungen und Wahrscheinlichkeit von Residualrisiken, um das verbleibende Betrugsrisiko nach der Umsetzung der Kontrollen zu berechnen.
- Berechnen Sie den Residualrisikowert, indem Sie die Folgen des Betrugsrisikos mit seiner Wahrscheinlichkeit multiplizieren (siehe Risikopriorisierungsmatrix in Anhang B).
- Verwenden Sie die Residualrisikowerte, um Risiken für weitere Maßnahmen zu priorisieren.

Schritt 4: Unterstützung der Betrugsrisiko-verantwortlichen sicherstellen

- Richten Sie bei Bedarf neue Kontrollen ein oder verbessern Sie bestehende Kontrollen.
- Sichern Sie sich die Unterstützung der Verantwortlichen für Betrugsrisiken und Kontrollen, um eine erfolgreiche Umsetzung zu gewährleisten.
- Stellen Sie die zeitnahe Umsetzung und Prüfung dieser Kontrollen mit Unterstützung der Stakeholder sicher.

3.2 Ergebnisse überprüfen und präsentieren

Anhand der Informationen aus dem Bewertungsprozess können Sie nun Ihren Bericht zur Betrugsrisikoanalyse erstellen. Wichtige Tipps:

- **Überprüfen** Sie den Inhalt des Berichts zusammen mit den wichtigsten Stakeholdern, um sicherzustellen, dass keine kritischen Risiken übersehen werden.
- **Halten** Sie den Bericht kurz und prägnant und verwenden Sie zur besseren Übersichtlichkeit und Verständlichkeit Tabellen und Diagramme.
- **Fügen** Sie eine Zusammenfassung hinzu, in der die wichtigsten Ergebnisse und Vorschläge ohne Fachjargon hervorgehoben werden, insbesondere wenn Sie die Budgetgenehmigung durch die Führungsebene einholen möchten.

Legen Sie den Bericht nach der Überprüfung den zuständigen Führungsgremien wie dem Vorstand, dem Risiko- und Prüfungsausschuss, der Führungsebene, anderen Mitarbeitern, der internen Revision und Fachleuten (Rechts-, Compliance-, Personalabteilung) zur Prüfung und Weiterverfolgung vor.

3.3 Maßnahmenplan und Kontrollpunkte

Weisen Sie auf Grundlage der Risikoanalyse jedem Risiko in Ihrem Maßnahmenplan einen **Betrugsrisikoverantwortlichen** zu, der für die Überwachung und Reaktion auf dieses bestimmte Risiko zuständig ist. Tragen Sie in einem **Risikoregister (siehe Anhang C1)** ein, welches Risiko welchem Verantwortlichen zugewiesen ist.

Die Betrugskontrollverantwortlichen sind für die Umsetzung und Aufrechterhaltung der Effektivität spezifischer Kontrollen verantwortlich.

Legen Sie Rollen und Verantwortlichkeiten klar fest (siehe Anhang C2).

Zu den bewährten Verfahren für die Pflege und Verwaltung Ihres Maßnahmenplans gehören:

- Stellen Sie sicher, dass Risikopläne für alle Stakeholder zugänglich und transparent sind und sie ganz einfach auf relevante Informationen zugreifen können.
- Führen Sie regelmäßige Besprechungen durch, um Ergebnisse zu kommunizieren und über Fortschritte zu berichten.
- Bieten Sie fortlaufende Schulungen an, um die Mitarbeiter über die neuesten Trends und Betrugsarten auf dem Laufenden zu halten.

4. Den Status quo verbessern

Die Meinungen darüber, wie häufig Unternehmen eine solche Risikoanalyse durchführen sollten, gehen auseinander. Letztendlich hängt die Häufigkeit von der Art und der Wachstumsentwicklung eines Unternehmens ab. Ein stabiles und reifes Unternehmen kann sich für einen jährlichen Prozess mit vierteljährlichen Überprüfungen entscheiden, während ein wachsendes Unternehmen möglicherweise regelmäßigere Risikoanalysen durchführen muss.

4.1 Analysieren, wo Sie gerade stehen

Wenn Ihr Unternehmen reift und an Größe und Komplexität gewinnt, müssen Sie möglicherweise Ihre Risikoanalysenmethodik anpassen und ein Echtzeit-Verständnis Ihres Risikoprofils entwickeln. Sie müssen außerdem Ihren Ansatz zur Identifizierung und Fokussierung auf vorrangige Risiken verfeinern. Ein Echtzeit-Dashboard, das Risiken und Kontrollen automatisch bewertet, mag futuristisch erscheinen, aber einige Unternehmen, mit denen wir gesprochen haben, stehen kurz vor der Implementierung eines solchen Systems.

Die meisten etablierten Unternehmen verfügen bereits über eine Art der Betrugsrisikoanalyse. Wenn dies bei Ihnen der Fall ist, können Sie diesen Best-Practice-Leitfaden nutzen, um die Durchführung, Umsetzung und kulturelle Verankerung Ihrer Betrugsrisikoanalyse im gesamten Unternehmen zu verbessern.

4.2 Sinnvolle Verbesserungen identifizieren

Das Rahmenwerk zur Betrugsrisikoanalyse bietet eine Möglichkeit, wichtige Maßnahmen zu priorisieren. Allerdings kann die erstmalige Ausführung einer solchen Aufgabe überwältigend sein, insbesondere wenn dabei viele Maßnahmen mit hoher Priorität zutage treten. Durch konsequente Priorisierung kann Ihr Unternehmen im Laufe der Zeit sinnvolle Verbesserungen bei der Betrugsrisikoanalyse erzielen. Wenn Ihr Unternehmen jedoch deutlich zu wenig in Kontrollen investiert hat, besteht die einzige Möglichkeit, diesen Rückstand aufzuholen, darin, Zeit, Energie und Ressourcen des Unternehmens in die Betrugsbekämpfung zu investieren.

Die Umsetzung einer ganzheitlichen Maßnahme kann Synergien zwischen mehreren Geschäfts- und Betriebsbereichen aufdecken und Möglichkeiten für Rationalisierungen und Effizienzsteigerungen aufzeigen. Beispielsweise stellte ein Unternehmen, mit dem wir gesprochen haben, fest, dass ein Bereich Prozesse zur Multi-Faktor-Authentifizierung eingerichtet hatte, die auch von anderen Bereichen übernommen werden konnten. Das Unternehmen zentralisierte daraufhin seine Betrugsbekämpfungsmaßnahmen, nachdem es im Rahmen der Risikoanalyse weitere Synergien aufgedeckt hatte.

5. Die Zukunft der Betrugsrisikoanalyse

5.1 Live-Dashboards

Einmal eingerichtet, bildet ein solider Risikoanalyseprozess eine Plattform für die Identifizierung, Bewertung, Beurteilung und Minderung neuer Betrugsrisiken, unabhängig davon, ob diese durch neue Betrugsbedrohungen oder die Einführung neuer Produkte und Dienstleistungen ausgelöst werden.

Mit zunehmendem Wachstum eines Unternehmens steigt jedoch in der Regel auch das Datenvolumen. Manuelle Risikoanalysen lassen sich nur schwer effektiv skalieren. Automatisierungstools können den Risikoanalyseprozess verbessern und die Abhängigkeit von manuellen Berichten verringern.

Eine große globale Bank teilte uns mit, dass ein Live-Dashboard für die Überprüfung von Betrugs-KRIs und -KPIs durch die Vorstandsausschüsse eingerichtet wurde. Dieses Dashboard ist automatisiert und wird von vielen Stakeholdern genutzt. Diese KRIs und KPIs können durch Fortschrittsupdates ergänzt werden, um Informationen über den Status der Risikominimierungsmaßnahmen und die sich verändernde Bedrohungslage zu liefern. Dadurch werden Informationen für Entscheidungsträger leichter zugänglich, sodass auch Nichtfachleute wichtige Daten schnell überblicken können (siehe Beispiel in Anhang D). Ein Dashboard kann die gesamte Risikomanagementlandschaft zusammenfassen und enthält:

- Änderungen in der Bedrohungslage, die Auswirkungen auf das Unternehmen haben
- eine Zusammenfassung der jüngsten Betrugsfälle und der daraufhin ergriffenen Maßnahmen
- die größten Betrugsrisiken aus dem Risikoanalyseprozess, gemessen anhand klar definierter Schlüsselrisikoindikatoren
- einen Plan der bestehenden Maßnahmen zur Risikominimierung mit den entsprechenden Verantwortlichkeiten, dem Umsetzungsstatus und den tatsächlichen Auswirkungen auf die Risikominderung

Ein gut aufgebautes Dashboard für das Betrugsrisikomanagement spiegelt die Risikobereitschaft des Unternehmens wider und wird automatisch mit konsistenten Daten aus dem gesamten Unternehmen in nahezu Echtzeit gespeist. Eine faktenbasierte Priorisierung hilft dabei, die Bemühungen auf die Bekämpfung der schwerwiegendsten und wahrscheinlichsten Betrugsrisiken zu konzentrieren. Umgekehrt können Unternehmen Kontrollen für weniger bedrohliche, weniger wahrscheinliche Risiken lockern oder ganz aufheben, um Ressourcen freizusetzen.

5.2 Silos aufbrechen

Das Betrugsrisikomanagement kann durch den Einsatz eines multidisziplinären Teams, das Ressourcen aus verschiedenen Geschäftsbereichen bündelt, effektiver gestaltet werden. Teammitglieder teilen in der Regel Geschäftsziele, die sich auf bestimmte Geschäfts- oder Kundenergebnisse und nicht unbedingt auf den Funktionsbereich beziehen, der ihrer Fachkompetenz entspricht.

Im Risikokontext könnte dies beispielsweise bedeuten, Experten aus den Bereichen Betrugsrisiken, Cyberrisiken und Geldwäscherisiken zusammenzubringen, um einen ganzheitlichen Risikomanagementansatz zu entwickeln. Dieses Team könnte die gleichen Techniken anwenden, die wir besprochen haben, um die Gesamtrisiken für das Unternehmen zu priorisieren.

6. Fazit

Die Betrugsrisikoanalyse findet in der Unternehmensrisikobewertung traditionell weniger Beachtung, was vor allem auf die Fokussierung auf betrugsbedingte Verluste zurückzuführen ist. Im Gegensatz zum AML-Sektor, der stark von der Einhaltung gesetzlicher Vorschriften geprägt ist, wird Betrug eher mit Diebstahl und Delinquenz in Verbindung gebracht. Diese Wahrnehmung ändert sich jedoch, da Länder wie Australien und das Vereinigte Königreich unterschiedliche Ansätze verfolgen und zunehmend der Betrugsrisikoanalyse Vorrang einräumen. In den USA legen die Regulierungsbehörden bei ihren Prüfungen zunehmend Wert auf die Betrugsrisikoanalyse, was auf eine Verlagerung des Schwerpunkts innerhalb des regulatorischen Umfelds hindeutet.

Unabhängig von regulatorischen Vorschriften bieten Betrugsrisikoanalysen einen ganzheitlichen und strukturierten Ansatz, von dem Unternehmen jeder Größe profitieren. Durch die systematische Identifizierung, Bewertung und Minderung von Betrugsrisiken können Unternehmen nicht nur ihre finanziellen Vermögenswerte schützen, sondern auch ihren Ruf wahren und das Vertrauen ihrer Stakeholder aufrechterhalten. Die Integration von Betrugsrisikoanalysen in das allgemeine Risikomanagement eines Unternehmens fördert einen proaktiven Ansatz, bei dem potenzielle Schwachstellen behoben werden, bevor sie ausgenutzt werden können. Dieser Ansatz stellt sicher, dass das Betrugsrisikomanagement mit den übergeordneten Strategien des Unternehmensrisikomanagements im Einklang steht, und fördert eine Kultur des Risikobewusstseins im gesamten Unternehmen.

Das wachsende Interesse der Regulierungsbehörden unterstreicht die Bedeutung von Betrugsrisikoanalysen, die über reine Compliance hinausgehen. Unternehmen, die diesen Wandel begrüßen, sind besser aufgestellt, um auf neue Betrugsbedrohungen zu reagieren, sich an regulatorische Änderungen anzupassen und robustere Risikomanagementpraktiken zu implementieren. Letztendlich ist eine gut durchgeführte Betrugsrisikoanalyse ein wichtiges Instrument zum Aufbau von Resilienz, das es Unternehmen ermöglicht, sich in einem zunehmend komplexen Risikoumfeld sicher zu bewegen.

7. Anhang A: Betrugstaxonomie

Betrugstaxonomie

Diese Betrugstaxonomie ermöglicht es Fachleuten für Finanzkriminalität, Betrugsfälle anhand von vier verschiedenen Phasen zu klassifizieren:

1. WER hat die Zahlung veranlasst?

2. WIE wurde der Betrug begangen?

3. WELCHE Taktik wurde angewendet?

4. WO fand der erste Verstoß oder Kontakt statt?

Außerdem können Fachleute eine Vielzahl von Details zum Betrug, zu seiner primären Typologie, zum Kanal, über den er begangen wurde, sowie zum Ausmaß der Verluste und zu den mit der Betrugsart verbundenen Fällen eingeben.

Siehe ACAMS-Betrugstaxonomie.

8. Anhang B: Risikopriorisierungsmatrix

Anhang B1: Risikopriorisierungsmatrix

Eintrittswahrscheinlichkeit	Schadenshöhe				
	Unbedeutend (1)	Geringfügig (2)	Mäßig (3)	Bedeutend (4)	Schwerwiegend (5)
Fast sicher (5)	MITTEL	HOCH	HOCH	SEHR HOCH	SEHR HOCH
Wahrscheinlich (4)	MITTEL	MITTEL	HOCH	HOCH	SEHR HOCH
Möglich (3)	NIEDRIG	MITTEL	MITTEL	HOCH	HOCH
Unwahrscheinlich (2)	NIEDRIG	NIEDRIG	MITTEL	MITTEL	HOCH
Selten (1)	SEHR NIEDRIG	NIEDRIG	NIEDRIG	MITTEL	MITTEL

SEHR NIEDRIG	2
NIEDRIG	3-4
MITTEL	5-6
HOCH	7-8
SEHR HOCH	9-10

Anhang B2: Risikomatrix-Schlüssel

Risikoniveau	Erforderliche Maßnahmen
SEHR HOCH	Das Risiko übersteigt die Risikotoleranz und den Risikoappetit des Unternehmens. Mindern Sie das Risiko sofort oder vermeiden Sie es. Führen Sie regelmäßige Überprüfungen durch und melden Sie das Risiko der Geschäftsleitung und allen relevanten Stakeholdern.
HOCH	Mindern oder vermeiden Sie das Risiko, es sei denn, der erwartete Nutzen der Aktivität überwiegt die Folgen des Risikos. Führen Sie regelmäßige Überprüfungen durch und melden Sie das Risiko allen relevanten Stakeholdern und der Geschäftsleitung nach deren Ermessen.
MITTEL	Das Risiko kann akzeptabel sein. Führen Sie regelmäßige Überprüfungen durch und melden Sie das Risiko innerhalb der relevanten Geschäftseinheit und den betroffenen Stakeholdern.
NIEDRIG	Das Risiko ist im Allgemeinen akzeptabel, muss jedoch überwacht werden, um sicherzustellen, dass sich die Risikoeinstufung nicht ändert.
SEHR NIEDRIG	Das Risiko ist akzeptabel.

9. Anhang C: Beispiel für ein Betrugsrisikoregister

Anhang C1: Beispiel für ein Betrugsrisikoregister

		Risikoidentifizierung			Kontrolleffektivität								Risikoidentifizierung			
		Risikoart	Risiko-beschreibung	Bestehendes Risikoniveau (siehe Risiko-priorisierungsmatrix)	Kontroll-maßnahmen	Kontrollarten	Kontrollen	Kontrollen eingeführt	Anzahl verhinderter Betrugsfälle	Betrugsbedingter Verlust (nach Kontroll-maßnahmen)	Anzahl nicht verhinderter Betrugsfälle	Ergebnis	Risiko-verantwortlicher	Kontroll-verantwortlicher	Risiko-prüfung	Zusätzliche Informationen
		Intern/ Extern	Beschreibung des Risiko und warum es analysiert wird	Sehr hoch/ Hoch/Mittel/ Niedrig/Sehr niedrig	Ja/Nein	Prävention/ Aufdeckung/ Reaktion	Mindernde Kontrollen zur Reduzierung des Risikos	Ja/Nein	Anzahl der durch die Kontrollen verhinderten Betrugsfälle	$	Anzahl der Betrugsfälle, die von der Kontrolle nicht erfasst wurden	(Eliminieren/ Reduzieren/ Akzeptieren)	Titel und Abteilung	Titel und Abteilung	Wöchentlich/ Monatlich/ Jährlich	
First-Party-Betrug	Kreditbetrug															
	Warenverlust während des Transports															
	Antragsbetrug															
	Gefälschte Dokumente															
	Antragsbetrug															
	Synthetische Identität															
	[Weitere Betrugsarten hinzufügen, die für die Geschäftstätigkeit Ihres Unternehmens relevant sind.]															
Second-Party-Betrug	Geldwäsche															
	Rückbuchungsbetrug															
	Geldwäsche mit Geschenkkarten															
	Betrug durch falsche Händler															
	[Weitere Betrugsarten hinzufügen, die für die Geschäftstätigkeit Ihres Unternehmens relevant sind.]															
Third-Party-Betrug	Übernahme von Konten															
	Identitätsdiebstahl															
	Autorisierte Push-Zahlungen infolge von Betrugsmaschen															
	Kompromittierung von Geschäfts-E-Mails/Phishing															
	[Weitere Betrugsarten hinzufügen, die für die Geschäftstätigkeit Ihres Unternehmens relevant sind.]															

Die Tabelle in Anhang C1 ist ein Beispiel für ein Risikoregister, in dem die Schritte und Überlegungen aufgeführt sind, die bei der Durchführung Ihrer Betrugsrisikoanalyse erforderlich sind. Dies ist eine Vorlage von ACAMS. Leser können das Format und den Inhalt entsprechend den geschäftlichen Anforderungen Ihres Unternehmens ändern.

Anhang C2: Anwendung an einem Beispiel

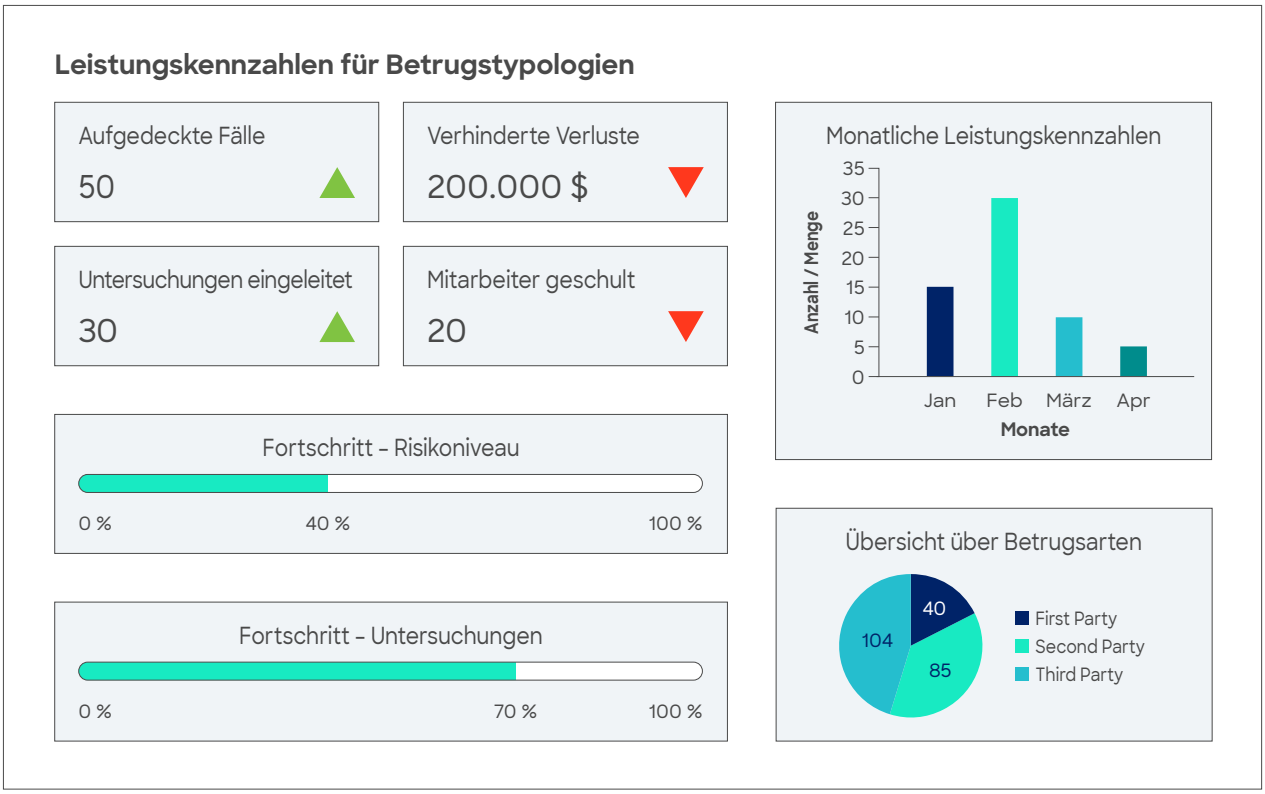
Im Folgenden wird anhand eines Beispiels ein Ansatz zur Einrichtung neuer Kontrollen für ein identifiziertes hohes Betrugsrisiko erläutert.

Identifiziertes Risiko	Ein Krimineller eröffnet ein Konto unter Verwendung einer synthetischen Identität (ID).
Bestehende Kontrollen	• Überprüfung anhand einer Datenbank für gefälschte IDs • Gemeinsame Nutzung von Informationen mit anderen Unternehmen • Dokumentenprüfung zur Bestätigung, dass das vom Kunden vorgelegte Ausweisdokument echt ist
Risikowert	7 = Hoch: Die Wahrscheinlichkeit, dass dies geschieht, ist aufgrund historischer Daten hoch und könnte mit dem Aufkommen künstlicher Intelligenz noch steigen. Die Folgen könnten schwerwiegend sein, wenn die Zahl der Vorfälle zunimmt.
Kontroll-vorschläge	Prävention: • Führen Sie eine Multi-Faktor-Authentifizierung ein, indem Sie mehrere Formen der Verifizierung verlangen, wie beispielsweise einen einmaligen Passcode, der an das Mobilgerät des Kunden gesendet wird. • Verwenden Sie die wissensbasierte Authentifizierung, um die Identität des Kunden zu überprüfen, indem Sie spezifische Fragen stellen, die nur der Kunde beantworten kann.
Risiko-verantwortlicher	Geschäftsführer
Kontroll-verantwortlicher	Leiter der Betrugsbekämpfung
Zeitrahmen	Vollständige Umsetzung bis Ende Dezember nächsten Jahres
Residual-risikowert	4 = Niedrig: Anzahl der Vorfälle und Verluste reduziert

Betrugsrisikoverantwortliche sind dafür zuständig, dieses spezielle Risiko zu überwachen und darauf zu reagieren. In der Regel handelt es sich dabei um leitende Führungskräfte.

Betrugsbekämpfungsverantwortliche sind für die Umsetzung und Aufrechterhaltung der Effektivität spezifischer Kontrollen zuständig. Es gibt also einen Betrugsrisikoverantwortlichen, aber möglicherweise mehrere verschiedene Kontrollen in Bezug auf dieses Risiko, für die die verschiedenen Unternehmensbereiche wie IT, Rechtsabteilung und Betrugsbekämpfung verantwortlich sind.

10. Anhang D: Beispiel für ein Dashboard zur Betrugsrisikoanalyse



Autoren und Mitwirkende

Autoren

Shilpa Arora, Head of AFC Products and Solutions, ACAMS

Joby Carpenter, Global Subject Matter Expert, Crypto and Illicit Finance

Florence Hui, Senior Manager, AFC Products and Solutions, ACAMS

Madiha Kanwal, Fraud Subject Matter Expert, ACAMS

Katy Worobec, Director, Azymus Consilium Fraud Consultancy

ACAMS möchte sich bei den folgenden Personen bedanken, die einen wichtigen Beitrag zu diesem Leitfaden geleistet haben:

Jonathan Arras, Senior Director, Fraud Product, Visa

Freddy Arthur, EMEA Fraud Strategy Leader, Nice Actimize

Mauriceo Castanheiro, Head of Product Strategy, Fraud Solutions, Verafin

Sally Felton, Director, Fraud Risk Management, BDO UK LLP

Edward Gilson, Senior Fraud Specialist, Vanguard

Kamlesh Harry, Director – Fraud Risk, Payment & Digital, Standard Chartered

Damian Hixson, Partnership Manager, CIFAS

Anthony Hope, Group Head of AML, CTF and Fraud Risk, National Australia Bank

Levent Kutluca, Head of Fraud, HSBC Asia Pacific

Katherine Odendaal, Director, Financial Crime, Fraud & Investigative Services, Guidehouse

Raymond Olsen, SVP, Director of Enterprise Fraud Management, Wintrust Financial Corporation

Vishnu Palaniappan, Director, Global Wholesale Fraud, HSBC

Dr. Durgesh Pandey, Partner, DKMS & Associates

Nisreen Sabri, Head Fraud Management – EMEA & Global Private Banking, HSBC Middle East

Anthony Shao, Partner (Fraud Detection and Investigation), Ernst & Young

Tobias van Kesteren, FCC Officer External Fraud/Business Change Manager, Rabobank

Kalyani Vasan, Partner, Strategy, Risk and Transactions, Forensic & Financial Crime, Deloitte

© 2025 ACAMS. Alle Rechte vorbehalten.
V28022025