Deloitte.

Künstliche Intelligenz in der Geldwäschebekämpfung

Von der KI-gestützten Alert Triage zu einer integrierten Analytics-Plattform für AFC

MAKING AN IMPACT THAT MATTERS since 1845

Effektivität des heutigen Transaction Monitoring

Die überwiegende Mehrheit der automatisierten Transaction-Monitoring-Systeme (TMS) basiert auf generischen Risikotypologien mit Regeln, die Schwellenwerte und weitere Parameter verwenden. In der Praxis generieren diese Regeln häufig eine große Anzahl von False Positive Alerts, die manuell bearbeitet werden müssen. Die bestehenden TMS inklusive der Alert-Generierung können durch den Einsatz neuer Technologien, die in der Lage sind, Regeln dynamisch und kundenspezifisch anzupassen, ohne dabei an Effektivität zu verlieren, deutlich verbessert werden.

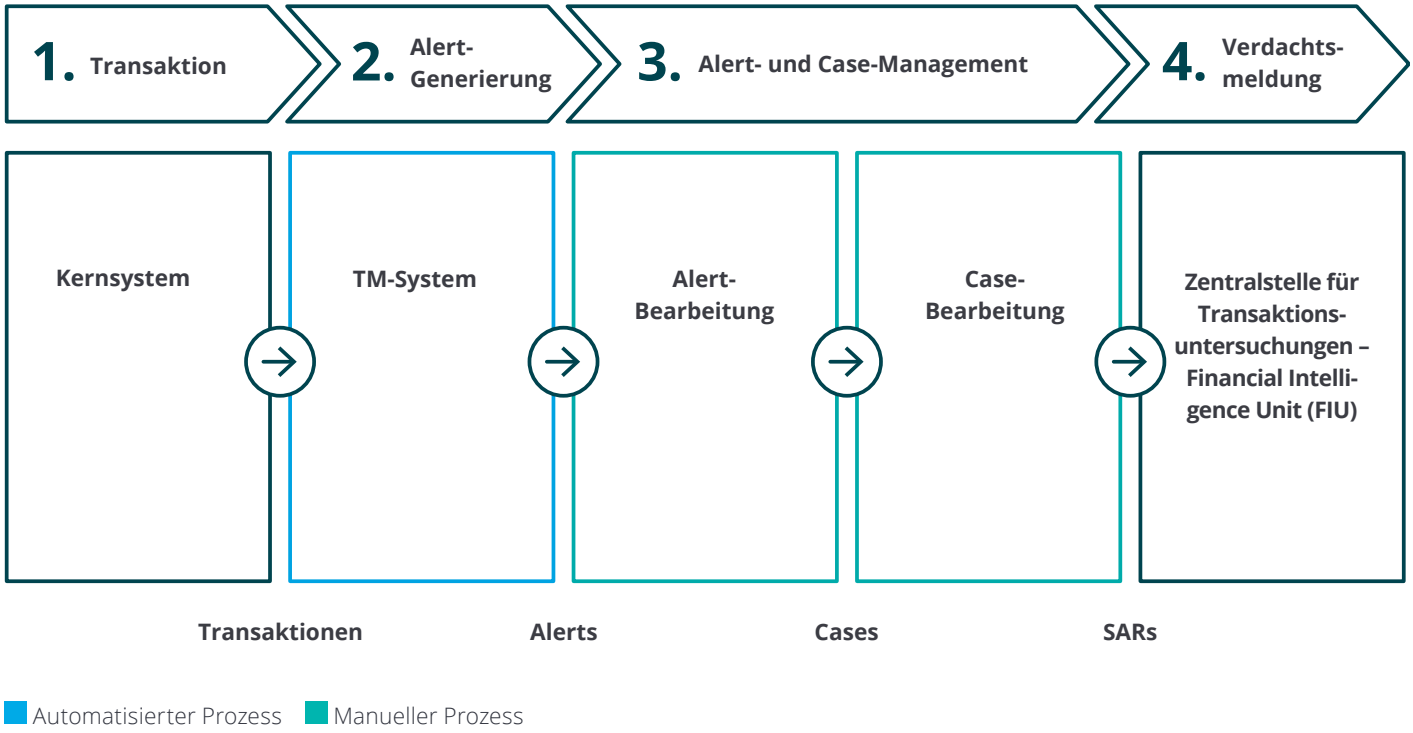
In der Praxis haben wir bei Banken die nachfolgenden Effektivitätsprobleme der aktuell verwendeten Systeme beobachtet.

Transaction Monitoring

Beim bestehenden Transaction Monitoring sollten Banken regelmäßig einen Above-the-Line- (ATL) und Below-the-Line- (BTL) Test durchführen, um die Modelle zu verbessern. Dadurch werden die Regeln und verwendeten Parameter einem Feintuning unterzogen. In der Praxis wird jedoch häufig kein vollumfängliches Backtesting von Alerts innerhalb von BTL-Tests durchgeführt. Dies ist unter anderem darauf zurückzuführen, dass hierfür eine groß angelegte Untersuchung von Transaktionen erforderlich wäre, die in der Produktionsumgebung im Rahmen der regulären Alert-Bearbeitung bereits geschlossen wurden. Ferner sind dynamische Testprozesse in vielen Fällen nicht in bestehende TMS integriert und Schwellenwerte werden nur durch beispielsweise jährliche ATL- und BTL-Tests angepasst.

Dieses unregelmäßige Feintuning sowie ein lückenhaftes Vorgehen bei der Implementierung und dem Backtesting neuer Typologien führen zu einem statischen System, das sich nur langsam an das sich stetig ändernde Verhalten von Kriminellen anpasst. Erkenntnisse aus dem Transaction Monitoring werden außerdem selten in Echtzeit im Kundenrisikoprofil aktualisiert bzw. fließen nicht in das Kunden-Scoring mit ein.

Abb. 1 – Klassischer Transaction-Monitoring-Prozess innerhalb eines regelbasierten Systems



Alert- und Case-Bearbeitung

Die Gründe, die zur Schließung von Alerts führen, sind häufig nicht standardisiert dokumentiert und werden daher im weiteren Verlauf auch nicht berücksichtigt. Zusätzlich stellen bei der Alert-Bearbeitung wiederkehrende Alerts ein Problem dar. Hierbei lösen identische Transaktionsmuster jedes Mal einen neuen Alert aus, auch wenn das Verhalten bereits als unverdächtig eingestuft wurde. Eine intelligente Lernfunktion ist in den meisten Systemen nicht enthalten.

Alerts-zu-SAR (ATSAR), Case-zu-SAR (CTSAR) und andere Metriken des Systems werden außerdem oft nicht in Echtzeit überwacht. Das Management ist so nicht in der Lage, den Fortschritt der Case-Bearbeitung oder Anpassungen des Systems anhand von Metriken wie Geldwäsche-Risikoexposition und Gesamtkosten des Geldwäscherisikos zu verfolgen.

Feedback zu einem Suspicious Activity Report (SAR) kann ferner normalerweise nicht von der FIU eingeholt werden und wird somit nicht zur Verbesserung der Effektivität des Systems verwendet.

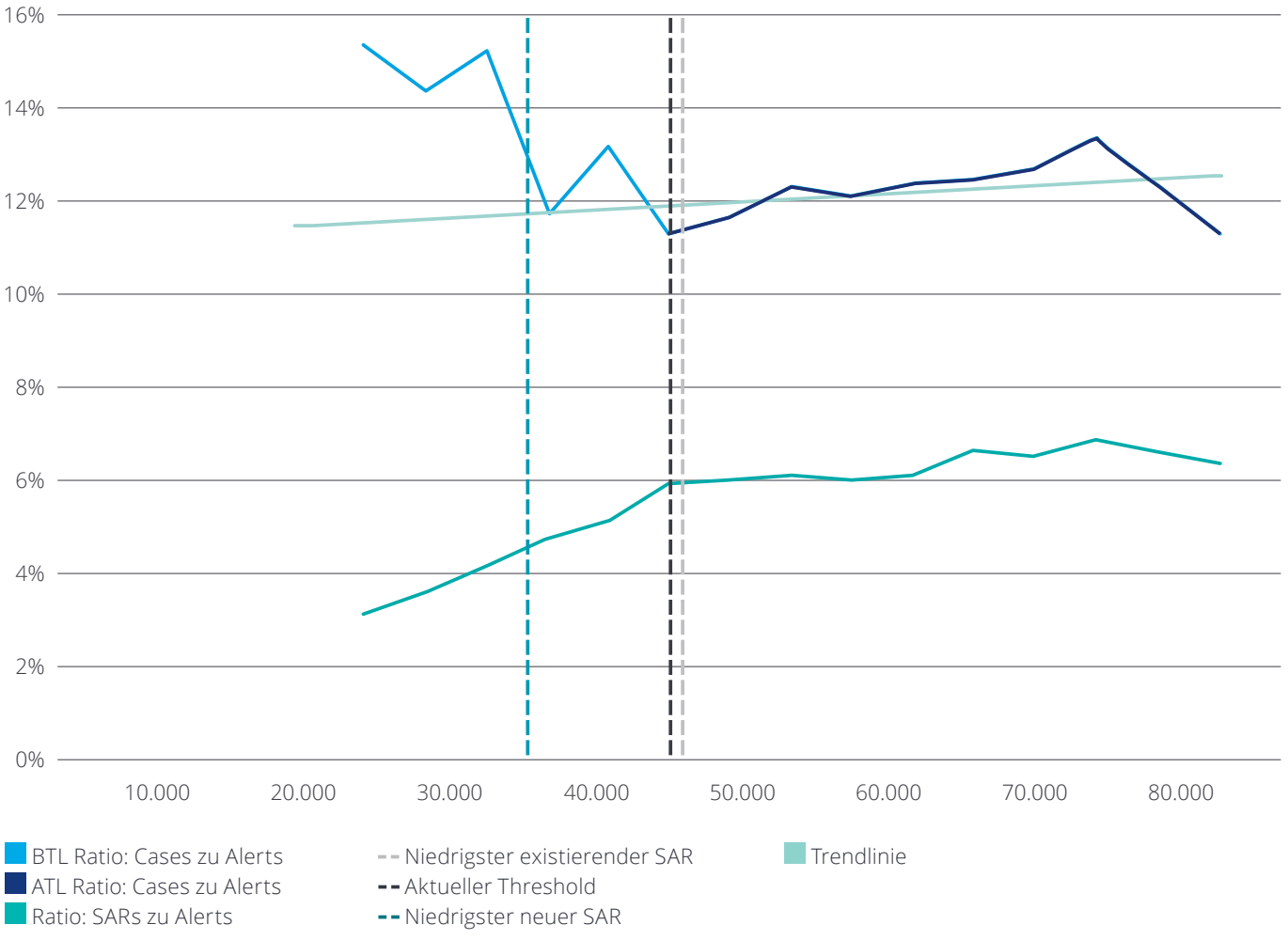
Anpassung Szenariomodell

Basierend auf bekannten und empfohlenen Typologien entwickeln Banken Regeln mit einzelnen Schwellenwerten. Sie legen dabei zunächst die Schwellenwerte fest und führen anschließend ATL- und BTL-Tests durch, um die Regeleffektivität und -effizienz zu bewerten. Die Schwellenwerte werden dann nach oben oder unten angepasst, um das Transaction Monitoring zu optimieren. Dieser Prozess, dargestellt in Abbildung 2, wird, ebenso wie die Erweiterung des Szenariomodells aufgrund neuer Typologien, häufig manuell durchgeführt und ist nicht formalisiert.

Dieser bestehende und in der Praxis allgemeingültige Optimierungsansatz beinhaltet jedoch viele Effektivitätsprobleme.

Die korrekte Schlussfolgerung und Ableitung von Maßnahmen aus den Ergebnissen eines ATL-Tests sind schwierig. Die Erhöhung des Schwellenwerts nach einem

Abb. 2 – ATL-/BTL-Testergebnis für eine einfache Regel



ATL-Test kann dazu führen, dass bestimmte verdächtige Transaktionen unentdeckt bleiben, obwohl die Erhöhung insgesamt zu einer Verbesserung der Alert-zu-SAR-Ratio führt. Die Bank steht damit vor dem Problem, den Effizienzgewinn gegen das Risiko abzuwägen. Unklar ist auch, wie Regeln und Schwellenwerte angepasst werden müssen, wenn sich der Risikoappetit der Bank ändert.

Eine mögliche Ineffektivität des Systems birgt zusätzlich das Risiko einer Ahndung durch die Aufsichtsbehörden (z.B. in Form einer Geldbuße). Aufsichtsbehörden aus dem In- und Ausland verhängen regelmäßig Strafen in Bezug auf verdächtige Transaktionen, die systematisch unentdeckt bleiben. Hohe Strafen werden in der Regel nicht für ein einzelnes Versäumnis bei der Erkennung und Meldung verdächtiger Aktivitäten verhängt, sondern vielmehr dann, wenn ein wiederkehrendes Muster auf eine schwache Kontrollumgebung hinweist. Inkorrekte Identifikation und Verarbeitung verdächtiger Alerts können außerdem zu einem Reputationsschaden führen, weswegen möglicherweise Kunden und andere Geschäftspartner verloren gehen.

Insgesamt gibt es mehrere theoretische und praktische Hindernisse bei der Quantifizierung der Kosten, die durch eine hohe False Negative Ratio entstehen können. Trotz eines kausalen Zusammenhangs der Kosten und der Effektivität des Systems mit Komponenten wie Strafzahlungen und Reputationsverlust sind diese schwierig quantifizierbar.

Entscheidungsmodelle bräuchten aber genau diese Schätzwerte bzw. Erwartungswerte von False-Positive- und False-Negative-Kosten, um damit eine mögliche „Verlustmatrix" erstellen zu können. Das Fehlen zuverlässiger Modelle für den Umgang mit False Negative Alerts stellt ein erhebliches Hindernis für die Implementierung eines umfassenden Entscheidungssystems für das Transaction Monitoring dar.

BTL-Tests von Regeln für TMS werden in vielen Rechtsordnungen entweder erwartet oder als bewährte Vorgehensweise angesehen. Eine Reihe von Faktoren beschränkt die Anwendung von BTL-Tests in der Praxis.

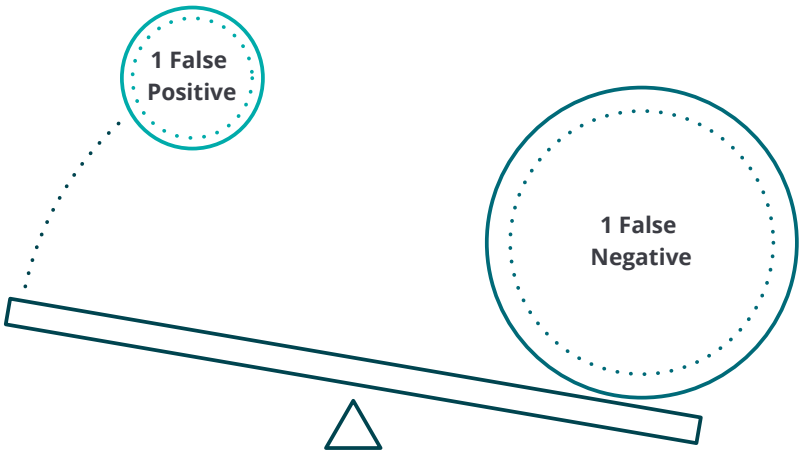
Diese führen zu einer hohen Anzahl an zusätzlichen Alerts, die manuell verarbeitet werden müssen. Viele Banken verfügen nicht über die nötigen Ressourcen, um solche Tests durchzuführen, da deren Mitarbeiter bereits mit der Bearbeitung der Alerts aus der Produktivumgebung beschäftigt sind.

BTL-Test sind aufgrund des hohen manuellen Aufwands sehr kostenintensiv. Es muss eine sehr große Anzahl von Transaktionen und Alerts bei verschiedenen Schwellenwerten überprüft werden. Darüber hinaus bestehen bei den Kontrollpersonen, die die BTL-Testergebnisse überprüfen, potenzielle Voreingenommenheit und Interessenkonflikte.

BTL-Tests führen in der Regel zu einer erneuten Bearbeitung in derselben Line of Defense, was ein Selbstüberprüfungsrisiko schafft. Falls ein zweites Team zur Verfügung steht, verfügt dieses oft nicht über ausreichend Erfahrung bezüglich der Kundenprofile und des Produktportfolios, um eine beträchtliche Anzahl neuer Alerts zuverlässig, effizient und konsistent zu bearbeiten. Das zuvor beschriebene Fehlen formalisierter Verfahren und entwickelter Positivlisten wirkt der Effektivität und Effizienz zusätzlich entgegen.

Darüber hinaus erfordern viele Geldwäsche-Typologien die parallele Anwendung und Umsetzung mehrerer Regeln, um eine zuverlässige Erkennung sicherzustellen. Die gleichzeitige Optimierung einer großen Anzahl von Parametern und verschiedenen Szenarios ist sehr anspruchsvoll. Eine weitere Herausforderung für Banken ist es, dabei das gewöhnliche vom ungewöhnlichen Kundenverhalten abzugrenzen. Diese Anforderung lässt sich nur schwer durch ATL-/BTL-Tests evaluieren.

Abb. 3 – False Negative Alerts haben das Potenzial hohe Kosten zu verursachen



Effizienz des heutigen Transaction Monitoring

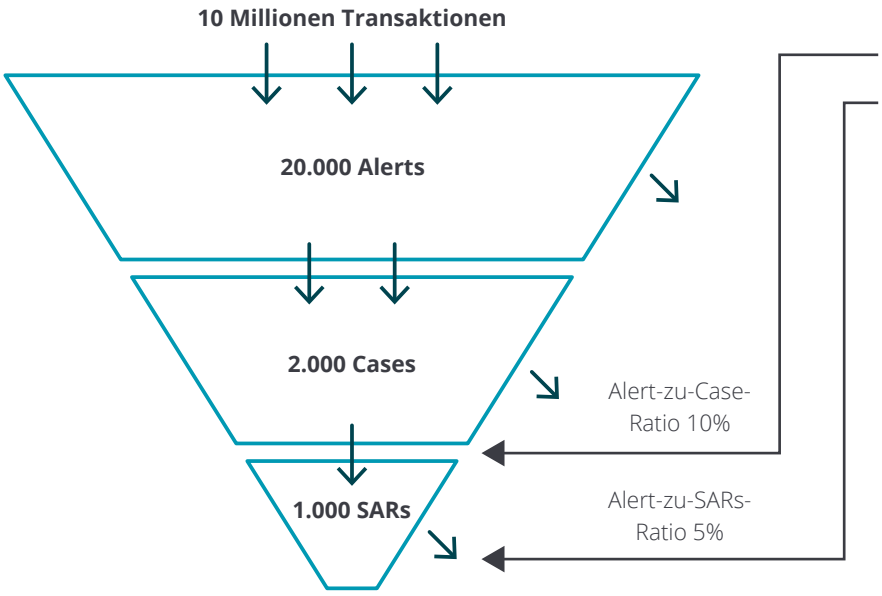
Die Regulierungsbehörden erhöhen permanent ihre Anforderungen hinsichtlich des Transaction Monitoring. Dies führt bei den Banken zu der Notwendigkeit, nach neuen und effizienten Lösungen zu suchen, da sonst mit steigenden Anforderungen auch die Kosten steigen.

Nehmen wir als Beispiel eine Bank, die jährlich 10 Millionen Transaktionen verarbeitet. Von den generierten 20.000 Alerts können 18.000 als False Positive Alerts unmittelbar und weitere 1.000 als False Cases geschlossen werden. Diese Bank hat somit eine 10-%-Alert-to-Case- und 5-%-Alert-to-SAR-Effizienzratio.

Mit dem Druck, die Erkennungsqualität zu verbessern, könnte sich die SAR-Effizienz verschlechtern, indem das TMS noch mehr False Positive Alerts generiert. Ein Anstieg der False Positive Alerts führt direkt zu erhöhten Personal- und Betriebskosten. In einem Umfeld, in dem der Druck wächst, das Transaction Monitoring kosteneffizienter zu gestalten, sind die derzeitigen Lösungen mittel- bis langfristig nicht zukunftsfähig.

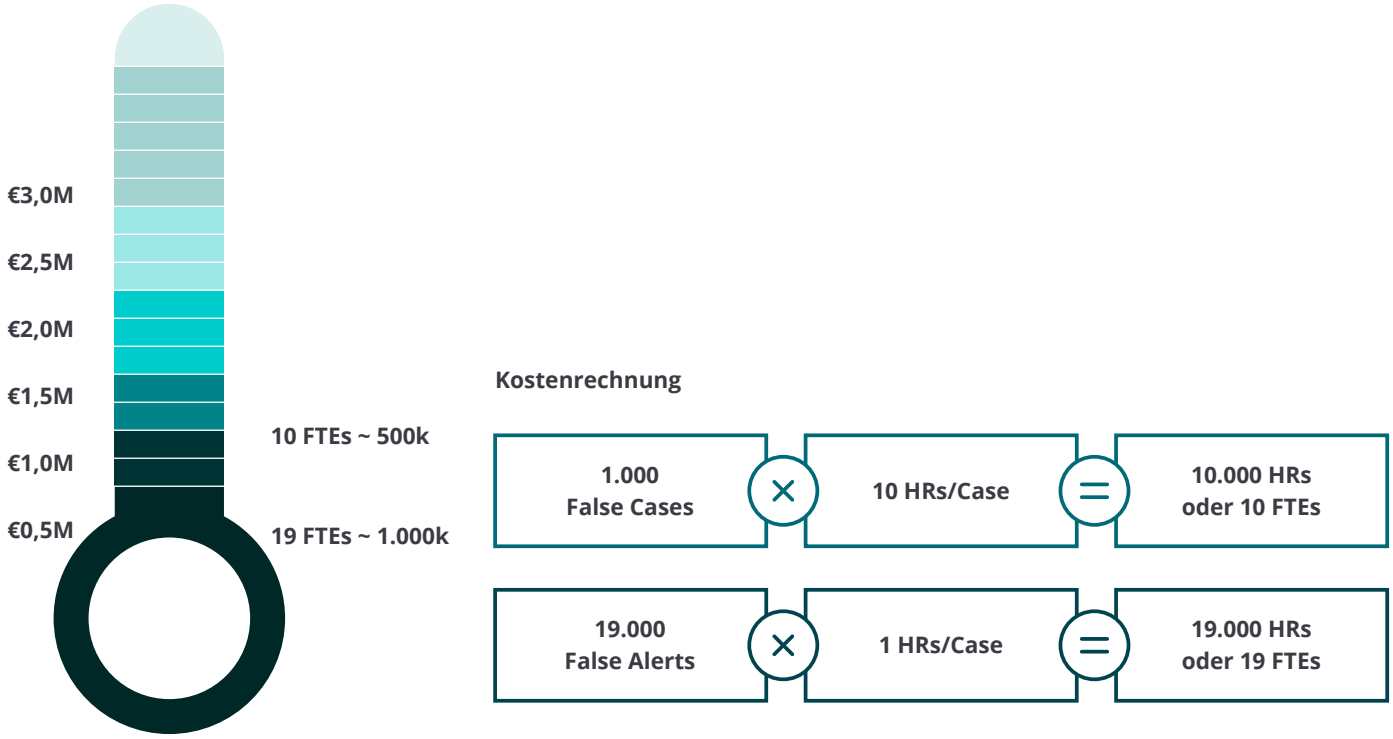
In diesem Beispiel schätzen wir die Personal- und Betriebskosten zum Betreiben eines TMS inklusive eines Case-Management-Systems für die Bearbeitung der 20.000 Alerts auf jährlich 1,5 Mio. Euro.

Abb. 4 – Effizienz beim Transaction Monitoring



	True Positive	False Postive
Alerts	1	19
Cases	1	1
SARs	1	n.a.

Abb. 5 – Kostenauswirkungen von False Positive Alerts beim Transaction Monitoring



Die Effizienz des Transaction Monitoring kann durch die Menge der Ressourcen bestimmt werden, die eingesetzt werden, um ein angemessenes Compliance-Niveau sicherzustellen. Ein wesentlicher Teil der Kosten sind Personalkosten innerhalb der 1st Line of Defense und der 2nd Line of Defense. Die Bearbeitungszeit sowie die Personal- und Systemkosten können identifiziert und berechnet werden. Mit diesen Informationen kann man die Gesamtkosten kalkulieren, um zu evaluieren, wie mögliche Initiativen zur Alert-Automatisierung die Effizienz verbessern könnten.

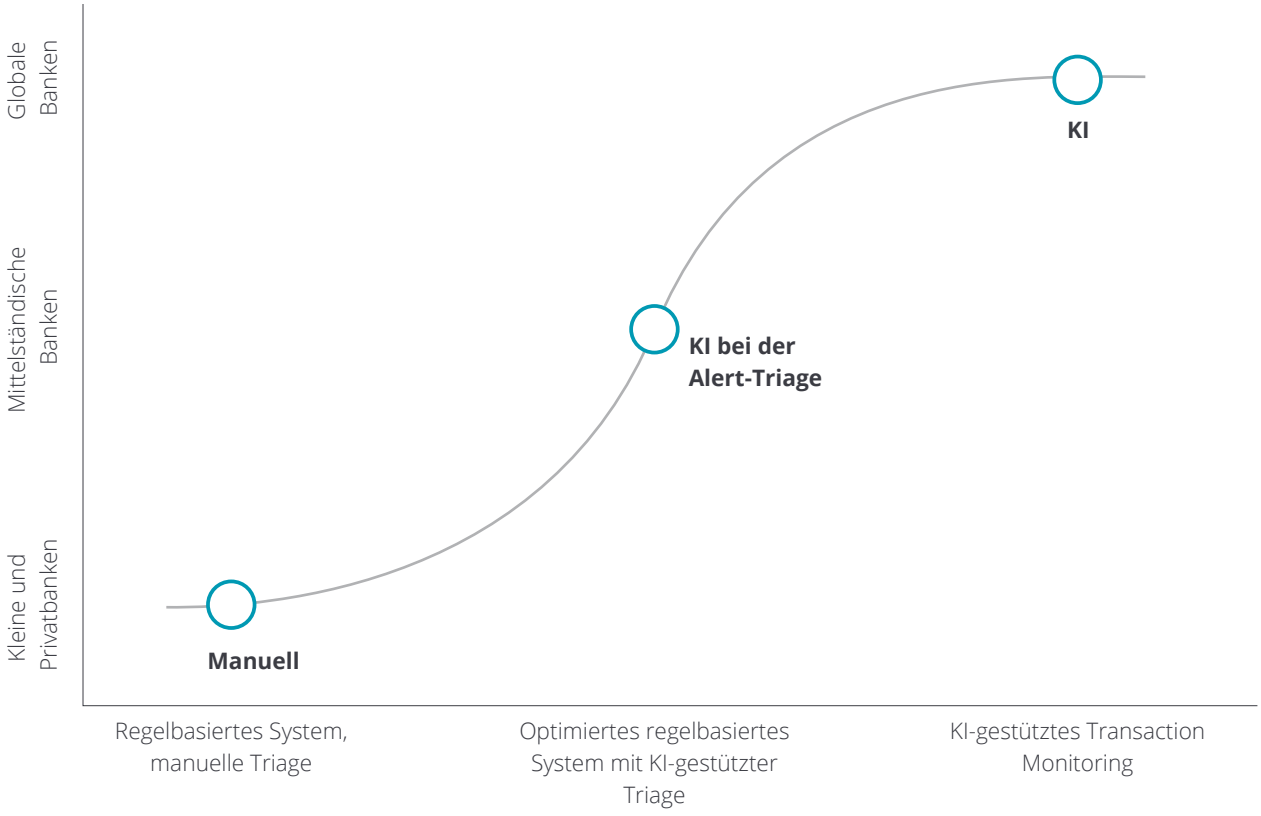
Setzen Banken in der Geldwäschebekämpfung Künstliche Intelligenz (KI) bereits aktiv ein? Das nächste Kapitel beschreibt ein Deloitte-Projekt, bei dem erfolgreich die False-Positive-Rate bei einer Bank um 40 Prozent reduziert werden konnte. Selbst für eine kleine Bank könnte eine solche False-Positive-Alert-Reduktion zu jährlichen Einsparungen von geschätzten 600.000 Euro führen. Investition und Implementierung eines KI-fähigen TMS können daher schnell zu einem hohen Return on Invest führen.

Aktueller Stand der KI im Transaction Monitoring

Die untenstehende Grafik veranschaulicht den aktuellen Stand bei der Einbindung von KI bzw. Machine Learning (ML) innerhalb des Transaction Monitoring. Die Praxis zeigt, dass aktuell vermehrt Finanzdienstleister versuchen, Use Cases unter Einbeziehung von KI in ihre Abläufe und Systeme zu integrieren. Die Zukunft des Transaction Monitoring liegt in der erfolgreichen Integration von KI bzw. ML in die ursprünglich regelbasierten Systeme. In einem solchen Fall würde die KI feststellen (oder eine interpretierbare Empfehlung an den Alert-Bearbeiter geben), ob eine bestimmte Transaktion als verdächtig eingestuft werden sollte. Ebenso könnte die Case Investigation entweder von einem Alert-Bearbeiter oder von der KI durchgeführt bzw. unterstützt werden. Unserer Erfahrung nach wird die Komplexität der Entwicklung einer solchen KI-Anwendung leicht unterschätzt. Bei einer großen Anzahl von Banken, insbesondere bei kleinen und mittleren Banken wurde bisher keine KI in die bestehenden Systeme integriert.

KI bei der Bearbeitung und Priorisierung von Alerts aus den regelbasierten TMS einzusetzen ist aufgrund der aktuellen Sichtweise auf das Thema bei Regulatoren und europäischen Banken durchaus eine Überlegung wert. Dadurch lassen sich False Positive Alerts im System schneller identifizieren und können effizienter bearbeitet werden. Die Alert-Bearbeiter haben so mehr Zeit zur Verfügung, um sich auf schwierige und komplexe Fälle zu fokussieren.

Abb. 6 – Der aktuelle Stand der KI im Transaction Monitoring



Case Study | internationale Großbank

Deloitte hat bei einer führenden asiatischen Bank in einem Pilotprojekt ein zweites, zusätzliches TMS implementiert. Die integrierte Lösung basiert auf dem Anti-Money-Laundering (AML) Framework der Bank, das die Prozesse „Know Your Customer", „Transaktionsüberwachung", „Name Screening" und „Payment Screening" umfasst.

Diese Lösung verwendet ein sekundäres Modul, um das bestehende, primäre regelbasierte System zu verbessern.

Das Modul enthält eine KI-Engine und dient als zusätzliche Einheit, um die Effektivität und Effizienz des TM-Systems zu erhöhen. Das Transaction-Monitoring-Modul fokussiert sich dabei auf die Erkennung neuer unbekannter verdächtiger Muster und priorisiert bereits generierte Alerts. Mithilfe der KI-Engine können die Regeln und Schwellenwerte innerhalb des TMS optimiert werden. Diese Optimierung wird durch die kontinuierliche und regelmäßige ATL-Hintergrundüberwachung des KI-Systems innerhalb des primären TMS erreicht, während die BTL-False-Negative-Hintergrundüberwachung zu Effektivitätsverbesserungen führt.

Transaction Monitoring
5% Anstieg der True Positives

Transaction Monitoring
40% Reduzierung der False Positive Alerts

Operative Effizienz
40% Steigerung der betrieblichen Effizienz

Case Study | eine Privatbank

Die Implementierung eines KI-basierten Moduls bei einer Bank mit einer kleineren Anzahl von Transaktionen kann zu gewissen Schwierigkeiten führen. Aufgrund der geringeren Anzahl an Transaktionen wird auch die Anzahl der Alerts, der zu bearbeitenden Cases und der daraus resultierenden Verdachtsmeldungen geringer sein. Aus Sicht der Data Science ist es schwierig, ein Machine-Learning-Modell mit einem kleinen Datensatz aufzusetzen. Das Modell könnte Schwierigkeiten haben, Alerts korrekt zu klassifizieren, da es nicht über ausreichend viele Trainingsbeispiele verfügt. Es würde auch dazu neigen, „Messfehler" zu generieren, d.h., es könnten nicht vorhandene Probleme und Abhängigkeiten identifiziert und die Aufmerksamkeit der Alert-Bearbeiter von realen Risikobereichen abgelenkt werden.

Um die Probleme zu überwinden, die in Verbindung mit kleinen Trainingsdatensätzen entstehen, hat Deloitte eine Technologie mit einer Reihe von Data-Science-Ansätzen entwickelt:

- Für gewöhnlich lernt das System aus viel größeren Datenmengen, die durch SARs oder untersuchte Cases erzeugt werden. Bei diesem Ansatz wird das System zusätzlich dadurch trainiert, dass die geschlossenen Alerts der Alert-Bearbeiter einbezogen werden.
- Solche Analystenaktivitäten sind in der Regel nicht formalisiert. Dementsprechend muss das System eine Prozesszuordnung durchführen, wobei Informationen verwendet werden, die im System gespeichert, aber nie verwendet werden, wie z.B. Aktivitätsprotokolle von Analysten oder ähnliche Daten.
- Normalerweise sind Klassifikatoren sogenannte überwachte Lernalgorithmen. Diese arbeiten bei sehr unterschiedlichen Daten wie dem Kundenaktivitätsmuster weniger effizient. Wir verwenden unüberwachte Lernalgorithmen, um Kunden und Transaktionen in homogenere Verhaltensgruppen zu unterteilen, und wenden die Klassifikatoren nur dort an.
- Alert Scores werden interpretierbar gemacht, sodass der Analyst alle Faktoren sehen kann, die das Geldwäscherisiko für eine bestimmte Transaktion erhöhen oder verringern. Obwohl Machine-Learning-Modelle, die für die Alert-Klassifizierung verwendet werden, dem Analysten initial keine Interpretierbarkeit anbieten, kann dies durch die Darstellung der Parameter im Case-Management-System erreicht werden.

KI-gestützte Alert-Triage-Systeme

US-Regulierungsbehörden gehörten zu den Ersten, die den Einsatz von KI in AML-Prozessen förderten. Im Dezember 2018 veröffentlichten die Federal Reserve, die Federal Deposit Insurance Corporation (FDIC), das Financial Crimes Enforcement Network (FinCEN), die National Credit Union Administration und das Office of the Comptroller of the Currency (OCC) das „Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing". Das Dokument bezieht sich speziell auf Künstliche Intelligenz im Anti-Financial-Crime-(AFC-)Bereich. Wir gehen davon aus, dass Regulierungsbehörden in anderen Jurisdiktionen diesem Beispiel folgen werden. Trotzdem erwarten wir, dass auch in einem Umfeld, in dem der Einsatz von KI bei Banken nicht nur akzeptiert, sondern Banken sogar dazu ermutigt werden, die meisten von ihnen es nicht eilig haben werden, ihre regelbasierten TM-Systeme durch KI-basierte zu ersetzen. Sofern die KI-Modelle nicht hinreichend qualitätsgesichert sind, werden sowohl die Banken als auch die Aufsichtsbehörden vorsichtig sein, menschlich-heuristische und menschliche Entscheidungsfindung in den AFC- und AML-Workflows zu reduzieren.

Um dieser Skepsis gerecht zu werden, befürwortet dieses Whitepaper einen Hybridansatz – wobei KI als Backup-System für das Transaction Monitoring eingesetzt wird. Dieses könnte parallel zum TM-Kernsystem arbeiten, ohne es zu ersetzen, sodass die menschlichen Kontrollen erhalten bleiben. Zusätzlich zum Real-Time-Scoring von Alerts schlagen wir die folgende Funktionalität für die Minimal Value Proposition (MVP) einer solchen Anwendung vor (s. Abb. 7).

Schwellenwertoptimierung und Dashboards sind im MVP enthalten, da diese wünschenswerte und leicht umsetzbare Elemente eines KI-fähigen Triage-Systems sind.

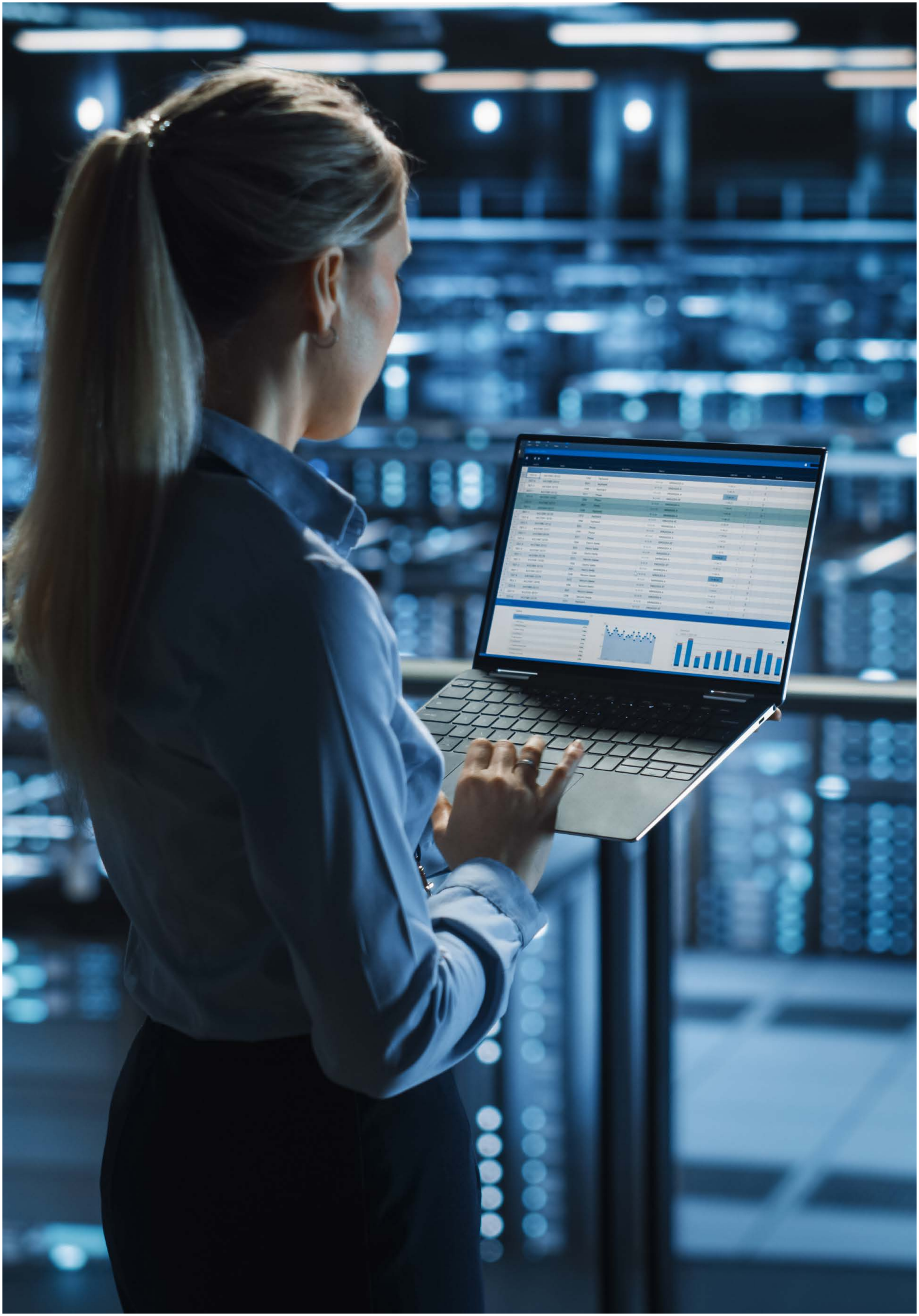
Abb. 7 – Funktionale Anforderungen an das Alert-Triage-System

Triage von Alerts
Spezifische Empfehlungen an das AML-Personal, wobei die endgültige Entscheidung auf menschlicher Ebene verbleibt

Positivlisten
Beobachtung und Einbezug von Informationen aus geschlossenen Alerts in die Erstellung von Positivlisten

Dashboard
Überwachung der ATSAR- und CTSAR-Effizienz und anderer Metriken des Systems, einschließlich der Gesamtkosten des Geldwäscherisikos

Schwellenwertoptimierung
Kontinuierliche ATL- und BTL-Optimierung von Regeln innerhalb des TM-Systems

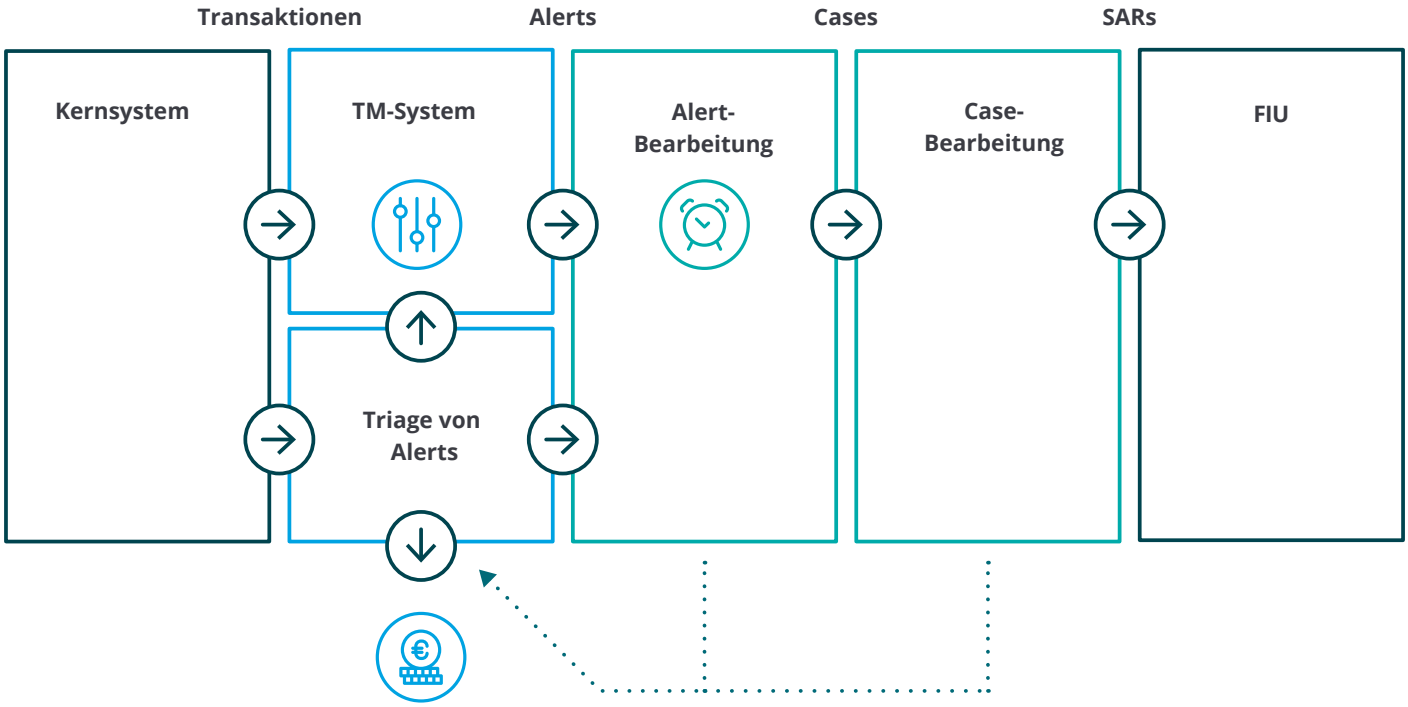


Die High-Level-Architektur für ein KI-fähiges Alert-Triage-System ist in Abbildung 8 dargestellt. Das Alert-Triage-System verwendet Algorithmen für überwachtes Lernen und Ähnlichkeitsmetriken, um die Transaktionen zu neu generierten Alerts mit denen zu vergleichen, die in der Vergangenheit als hohes Risiko eingestuft wurden. Eine solche Analyse müsste sonst manuell durchgeführt werden, indem jede Transaktion den gesamten Alert-Investigationsprozess durchläuft.

SARs wurden bewusst aus der Lernschleife ausgeschlossen, da es typischerweise zu wenige solcher Transaktionen im Trainingsset gibt, als dass die überwachten Lernalgorithmen daraus zuverlässig lernen könnten.

Ein solches System kann umfangreichere Eingaben verarbeiten als aktuelle Transaction-Monitoring-Systeme. Es könnte z.B. die gesamte Transaktionshistorie des Kunden sowie extern generierte Daten zu dem Kunden oder der Gegenpartei verarbeiten und in das Transaction Monitoring einbeziehen.

Abb. 8 – Die Lernschleife bei der Alert Triage



Auf dem Weg zu einer Analytics-Plattform für AFC

Ein KI-fähiges Alert-Triage-System könnte als erster Baustein für eine integrierte Analytics-Plattform für sämtliche AFC-Anwendungen dienen. Eine solche Plattform sollte jedoch, auch wenn sie zunächst nur als additive Komponente innerhalb der AML-Funktion konzipiert wäre, erweiterbar und zukunftssicher sein. Mit anderen Worten, sie muss die Erwartungen an Daten im modernen Banking erfüllen. Basierend auf unserer Erfahrung haben wir einige dieser Prinzipien in Abbildung 9 formuliert.

Datenmanagement in der Bank

Eine der Säulen des modernen Datenmanagements ist eine gemeinsame Datenarchitektur über Risiko- und Kundendomänen hinweg. Sie kombiniert die Kundenansicht nach umsatzgenerierenden Faktoren und Risikofunktionen, weshalb von einer 360°-Ansicht gesprochen werden kann. Dieser Ansatz birgt jedoch die Gefahr, dass ein effektiver Datenaustausch aufgrund von objektiven Interessenkonflikten zwischen organisatorischen Einheiten verhindert wird.

Es kann beobachtet werden, dass selbst innerhalb der Risikofunktionen Kundendaten nicht immer fehlerfrei ausgetauscht werden. Als Beispiel könnte man hier den Bereich Kreditrisiko und AFC nennen. Aus diesem Grund befürworten wir das Data-as-a-Product-Konzept, bei dem einzelne Domains für ihre Datenbestände verantwortlich sind, aber für die holistische Wertschöpfung von der Bank Anreize erhalten.

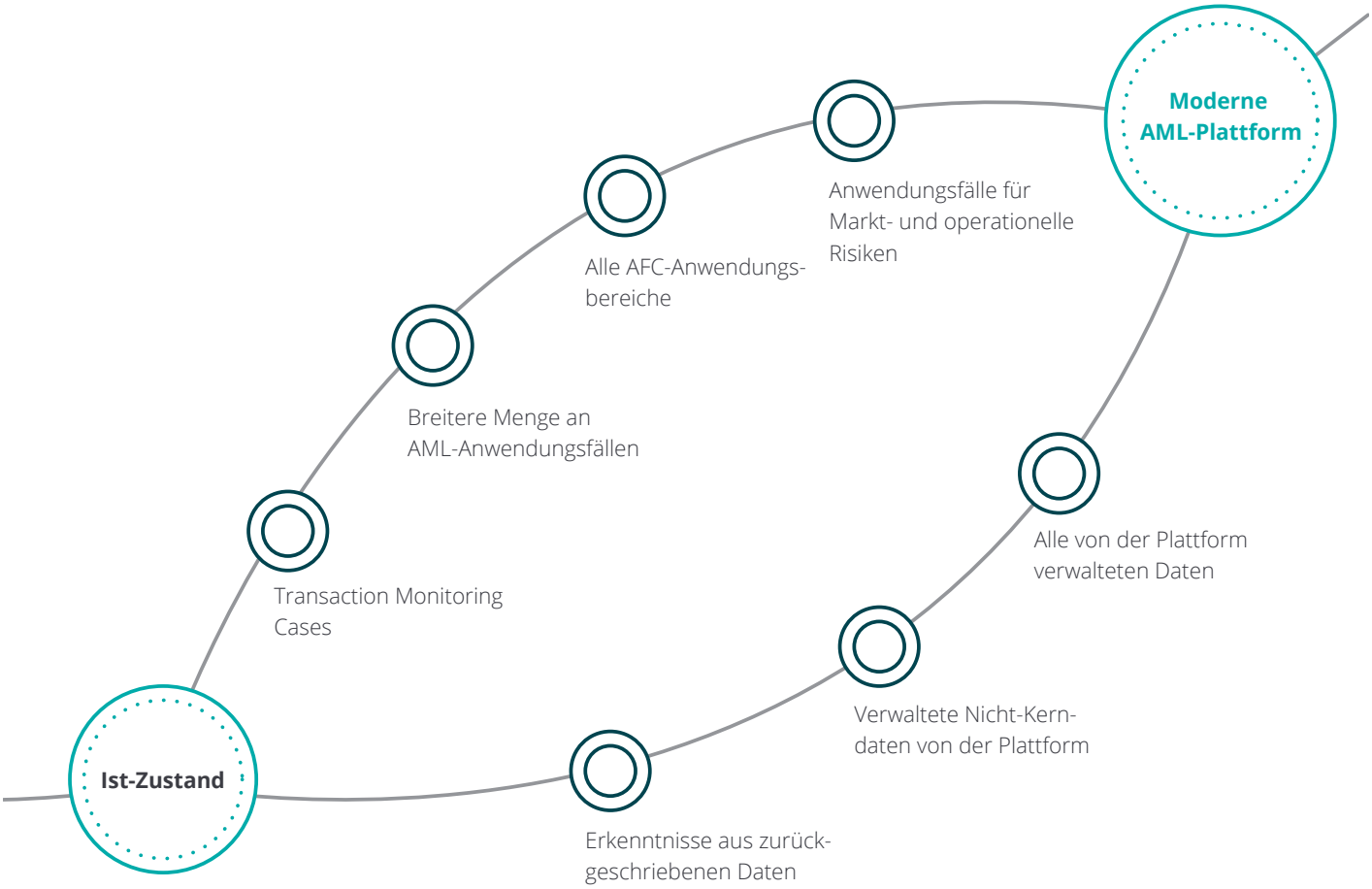
Der traditionelle Ansatz beim Aufbau einer Datenplattform besteht darin, dass erhebliche Vorabinvestitionen erforderlich sind, bevor die Bank die Vorteile realisieren kann. Außerdem verfügt sie möglicherweise nicht über die notwendige Reife und Kompetenz, um alle grundlegenden Elemente auf einmal aufzubauen.

Um das Risiko von Kosten- und Zeitüberschreitungen zu minimieren, wird stattdessen ein modularer Ansatz empfohlen, der die AFC-Daten- und Analytics-Plattform stufenweise entwickelt.

Abb. 9 – Erwartungen an Daten im modernen Banking

1. Gemeinsame Kundendaten nach Risiko und Umsatz	2. Datenmanagement	3. Datenaustausch
• Personalisierung und Risikomanagement auf der Grundlage einer gemeinsamen Ontologie • Vollständiger Überblick über finanzielle und operative Risiken • Ontologie der Risikofaktoren, die ähnliche Risiken für verschiedene Kunden erfasst • Wiederverwendung von KI-Modellen in verschiedenen Bereichen (z.B. die Abwanderungsneigung, die sowohl bei der Kundenbindung als auch bei NSF/Reifegradleitern verwendet wird)	• Ermöglichung des Konzepts der „Column Owners" für den gesamten Datenfluss • Speicherung von Daten vor Ort/in der privaten Cloud und Tokenisierung von Daten bei der Übertragung und Modellierung • Hybride Architektur, die plattformübergreifend die volle Leistung moderner KI-/ML-Stacks ermöglicht • Erfüllung gesetzlicher und gesellschaftlicher Anforderungen an die Integrität von Daten und Modellen	• Angleichung von Wertschöpfung und -steigerung in der gesamten Wertschöpfungskette/im „Ökosystem" • Bessere Kundeneinblicke und Anwendungsfälle bei gleichzeitigem Verzicht auf Cookies von Dritten • Austausch von Erkenntnissen zwischen zwei Organisationen, ohne Daten auszutauschen • Senkung der Transaktionskosten für den Datenaustausch (Daten- und Modellmarktplätze) • Senkung der Kosten von Datendrittanbietern

Abb. 10 – Übergang zu einer AFC-Datenplattform



Stufenweiser Ansatz

Abbildung 10 veranschaulicht den phasenweisen Ansatz zum Aufbau einer Analytics-Plattform für die AFC-Funktion. Die Legacy-Banking-Technologien umfassen in der Regel eine Vielzahl von eigenständigen Anwendungen im AFC-Bereich, die Informationen über APIs austauschen, wie z.B. die Systeme für Transaction Monitoring und für das Case-Management. Der Übergang dieser Legacy-Architektur zu einer modernen Architektur erfolgt auf zwei Ebenen:

- Die Verantwortung für die Verwaltung der Daten geht nach und nach von eigenständigen Anwendungen auf die Plattform über. Zunächst werden Ergebnisse und Informationen aus analytischen Modellen noch in Anwendungen zurückgeschrieben. Im nächsten Schritt werden dann alle oder die meisten Daten innerhalb der Plattform selbst verwaltet. Außerdem wird auch die Datenstruktur aller Microservices, die auf der Plattform erstellt werden, auf dieser verwaltet.

- Datenbestände und Use Cases werden dabei modular entwickelt, sodass sie mit jedem neuen Element verbunden und integriert werden. Die Architektur wird durch Erkenntnisse ergänzt, die von vorhergehenden Datenbeständen generiert werden.

Schrittweiter Aufbau von AFC Use Cases

Abbildung 11 veranschaulicht, wie die Verantwortung für die Verwaltung der Daten von einzelnen Anwendungen auf die integrierte Plattform übergeht.

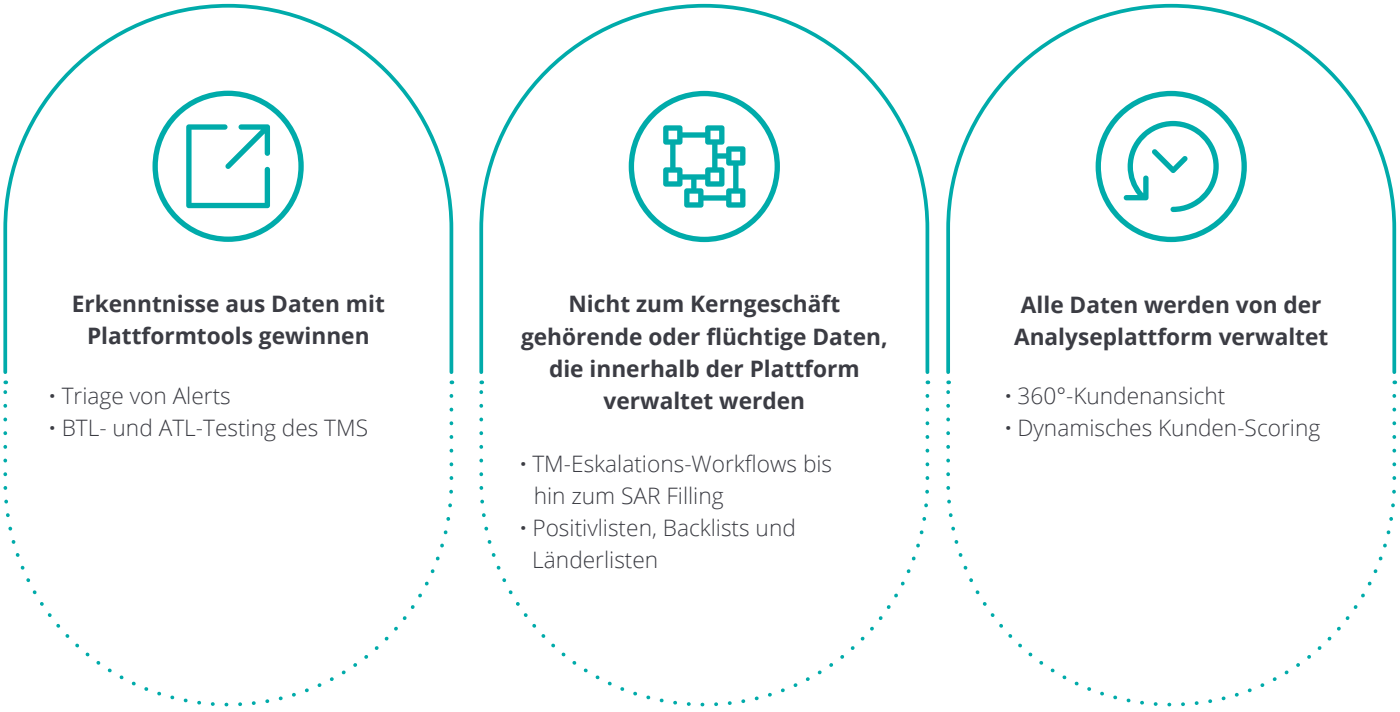
Im KYC-Prozess basieren Stand-alone-Anwendungen normalerweise auf einem hart codierten System, welches regelmäßig manuell auf Basis von neuen Informationen oder einem erweiterten Due-Diligence-Prozess (EDD) aktualisiert wird.

Kundentransaktionen oder Transaktionsuntersuchungen tragen in der Regel wenig dazu bei, die Sicht auf das Kundenrisiko zu ändern. Herkömmliche Transaction-Monitoring-Systeme sind nicht darauf ausgelegt, solche Erkenntnisse zu erfassen und bei der Bewertung des Kundenrisikos einfließen zu lassen, weil diese ein separates System sind.

Um sicherzustellen, dass die Ergebnisse des Transaction Monitoring in das AML-Risikoprofil des Kunden einfließen, müssen diese Informationen dynamisch in der Kundendatei als Output der KI-Anwendung aktualisiert werden, welche die Kundenrisikobewertung durchführt. Ebenso sollte sich ein erhöhtes Kundenrisiko auf die Tiefe der Überwachung und auf eventuelle Untersuchungen auswirken. Kunden, Transaktionen, Untersuchungen und Gegenparteien sind alles Objekte, welche in der AFC-Datengrundlage enthalten sein sollten. Sie beeinflussen sich alle gegenseitig, weshalb sich dies in den Daten widerspiegeln sollte. Eine solche dynamische Struktur ist die Kernanforderung an eine effektive Datenarchitektur für AFC.

Auf der nächsten Seite zeigen wir, was die Erwartungen an eine moderne Daten- und Analytics-Plattform für AFC sein sollten.

Abb. 11 – Die Verantwortung für das Datenmanagement geht auf die Plattform über



Erwartungen an eine integrierte AFC-Analytics-Plattform

Die Fähigkeit, Out-of-the-Box-Lösungen mit Eigenentwicklungen zu kombinieren. Eine gute Plattform beinhaltet einfache Use Cases, die für den AFC-Bereich relevant sind, sich aber gleichzeitig beliebig erweitern lassen.

Entwicklungsumgebung mit Low-Code-Funktionalitäten, welche es den Mitarbeitern der Fachabteilungen auch ohne Programmier- oder Datenbankkenntnisse ermöglicht, zumindest einfache Analysen durchzuführen.

Vollständig regulatorisch konform mit der Fähigkeit, bestehende und künftige Vorschriften in Bezug auf KI zu erfüllen, einschließlich der bevorstehenden EU-Richtlinie zu KI.

Data-Fabric-Architektur zur Gewährleistung bidirektionaler Datenflüsse zwischen mehreren AFC- und Risikoanwendungen einschließlich solcher, die auf der Plattform entwickelt wurden, und Anwendungen von Drittanbietern. Sie unterstützt nicht nur das Lesen von Daten aus Anwendungen, sondern auch das Schreiben.

Der Implementierungsansatz für Datennetzwerke, einschließlich seiner Schlüsselelemente wie Data as a Product, wobei das Eigentum an Datenressourcen in den jeweiligen Domänen innerhalb der Organisation verbleibt, die übergreifenden Nutzungsmöglichkeiten jedoch weit über die Risikofunktion und die Risikotechnologieteams hinausgehen.

Möglichkeit der integralen Umstellung, sodass ein zunehmender Teil der Daten direkt über die Plattform verwaltet wird und somit einzelne AFC- und Risikoanwendungen graduell ersetzt werden.

Modulare Implementierung mit komplexeren Datenbeständen und Use Cases, die auf weniger komplexen aufbauen.

Gemeinsame Datenarchitektur über Risiko- und Produktbereiche hinweg. Sie könnte zunächst als eine Architektur für alle Risikobereiche (z.B. 360°-Kundenansicht) erstellt und anschließend erweitert werden, um weitere Use Cases für andere Fachbereiche abzudecken.

Fördert eine eindeutige Kunden-ID-Kultur; einheitliche Kunden- und Ultimate-Beneficial-Owner-Lösung innerhalb der Plattform.

Dynamische Datenarchitektur, die nicht hart codiert ist und es ermöglicht, dass neue Daten und neue Erkenntnisse das Verständnis von Risiken kontinuierlich erweitern.

Zukunftsfähige Technologie, die alle bestehenden und zukünftigen KI Use Cases ermöglicht, einschließlich wachsender Bereiche wie die Analyse auf Basis von Graphdatenbanken.

Ihre Ansprechpartner

Martin Hirtreiter
Anti-Financial Crime Advisory
Tel: +49 69 75695 7059
mhirtreiter@deloitte.de

Julian Koller
Anti-Financial Crime Advisory
Tel: +49 69 75695 6385
jkoller@deloitte.de

Janina Uspelkat
Anti-Financial Crime Advisory
Tel: +49 40 32080 5555
juspelkat@deloitte.de

Deloitte.

Stand 03/2023