Anti Financial Crime:
Aufgabe für Management und IT

PUBLI-INTERVIEW

actico
Smarter Decisions

Bei der Prävention von Financial Crime gibt es nicht immer regulatorische Vorgaben. Finanzinstitute müssen Kunden und sich selbst schützen.

Sven Feddersen,
Project Director bei der ACTICO GmbH in Immenstaad am Bodensee/Deutschland, begleitet Finanz-institute bei der Implementierung von Compliance- und Client-Management-Systemen. Er ist Ansprechpartner für fachliche und technologische Fragestellungen rund um Anti-Geldwäsche, Marktmissbrauch, Embargo-Überwachung und andere regulatorische Themen.

Wie gut sind in Ihren Augen Schweizer Finanzinstitute gegen Financial Crime gerüstet, und wo sehen Sie die grössten Herausforderungen?
Wir sehen grosse Unterschiede, da manche fachliche Disziplinen sehr viel etablierter sind als andere. Beispiel «Geldwäscherei»: Hier kann mittlerweile auf eine langjährige Historie zurückgeblickt werden. Bei den beteiligten Parteien (Institute, Prüfungsgesellschaften, Aufsicht) gibt es Erfahrungswerte und einen gewissen Konsens im Hinblick auf die angemessenen Prozesse und Massnahmen. Im Mittel sind die Banken daher zu diesem Thema gut aufgestellt. Bei den implementierten IT-Lösungen stellt sich allerdings teilweise die Frage nach einem Generationswechsel, z.B. weil die ursprünglich eingeführten Systeme bezüglich Datenmengen und Komplexität der Prüfungen an ihre Grenzen stossen.

Anders sieht es hingegen oft bei kriminellen Handlungen aus, die sich gegen die Bank selbst oder gegen ihre Kunden richten und bei denen bislang kein vergleichbarer regulatorischer Druck bestand. Dort sind die Lösungswege weniger vorgezeichnet, und die Unsicherheit über die richtige Herangehensweise ist grösser.

Was müssen heutige Anti-Financial-Crime-Lösungen standardmässig abdecken? In welchen Bereichen sehen Sie zusätzlichen Investitionsbedarf?
Eine gute Software-Lösung muss vor allem flexibel genug sein, um den Bedürfnissen des einzelnen Instituts gerecht zu werden. Dies gilt zunächst für die erstmalige Einführung eines solchen Systems, bei der z.B. Überwachungsszenarien definiert bzw. angepasst werden. Basis für das Aufsetzen der Lösung sind die spezifischen Risiken, die aus dem konkreten Geschäft der Bank abgeleitet werden. Hohe Flexibilität ist aber auch danach erforderlich, um auf veränderte Situationen und Anforderungen zügig reagieren zu können. Die notwendigen Erweiterungen der Prüfungs- und Bewertungslogik müssen unabhängig von den sonst üblichen Release- und Einführungszyklen der eigenen IT möglich sein.
Den grössten Investitionsbedarf sehen wir bei der Umsetzung von präventiv wirkenden Lösungen. Anders als beim klassischen Monitoring, das eine Art «elektronischer Prüfspur» darstellt, sind zur aktiven Abwehr von kriminellen Handlungen in der Regel Eingriffe in operative Prozesse und IT-Systeme der Bank erforderlich. Und die sind mit Aufwand und Kosten verbunden.

Wird es künftig vermehrt Anti-Financial-Crime-Lösungen aus der Cloud geben?
Wir stellen bei unseren Kunden aktuell noch grosse Zurückhaltung fest, trotz des gestiegenen Kostendrucks. Viele Funktionen lassen sich nicht ohne Weiteres gleichwertig auch als Service in der Cloud bereitstellen. Problematisch sind vor allem Anwendungsfälle, in denen sehr umfangreiche oder aber schützenswerte Daten an den jeweiligen Dienstanbieter zu übermitteln

Quelle: Interview mit der Schweizer Bank, der führenden Fachzeitschrift für Führungskräfte im Bankwesen der Schweiz.

wären. Ist etwa eine sehr lange Datenhistorie zu analysieren, so erfordert dies die Übermittlung und ggf. Fortschreibung dieser Informationen in der Cloud. Und: Selbst ein einfacher Abgleich von Personendaten und einschlägigen Listen (z.B. PEPs) im Rahmen der Kundenannahme bedeutet im Fall einer Cloud-Lösung, dass Informationen zu einem potenziellen Kunden der Bank an einen externen Service Provider übertragen werden. Dies muss durch ein Institut stets bedacht und bewertet werden.
Chancen für kommerzielle Cloud-Lösungen sehen wir daher am ehesten in speziellen Anwendungsbereichen, bei denen Erkenntnisse auch aus mengenmässig begrenzten und anonymen Daten gewonnen werden können. Diese sind in ihrer Anzahl jedoch vermutlich eher begrenzt.
Was wir hingegen erwarten, ist eine verstärkte Zusammenarbeit der Finanzinstitute untereinander in «Community Clouds», d.h. den aktiven Austausch von technisch nutzbaren Daten, etwa zur Betrugsprävention. Im Vordergrund steht dabei weniger der Aspekt der Kostenoptimierung als die Ermöglichung qualitativ besserer Lösungen durch die Nutzung von Informationen im Verbund. Vorbedingung hierfür ist allerdings die rechtliche Klärung allfälliger Fragen des Datenschutzes.

Was sollten Banken zusätzlich unternehmen, um die Kultur eines Risikobewusstseins zu stärken und Compliance-Anforderungen zeitnah umzusetzen?
Compliance erschöpft sich nicht im Betrieb von IT-Systemen. Letztere können durch Automatisierung zusätzliche Erkenntnisse liefern und die formale Einhaltung von Regeln gewährleisten. Die Nutzung dieser technischen Möglichkeiten ist jedoch immer nur ein Baustein in einem Paket von Massnahmen zur Sicherstellung der Compliance und der Abwehr von kriminellen Handlungen. Ebenso wichtig ist etwa die Definition und Fortschreibung der erforderlichen Prozesse sowie die Erstellung von Weisungen und praxisbezogenen Handbüchern für die tägliche Arbeit. Um den einzelnen Mitarbeiter aber wirklich abzu-

"Software-Lösungen alleine reichen nicht aus, um compliant zu sein und um Bedrohungen durch kriminelle Handlungen von aussen und von innen abzuwenden."

holen, braucht es vor allem eine glaubhafte und gelebte Verpflichtung auf die eigenen Policies auf allen Ebenen des Managements. Dies gilt insbesondere für ein besonders heikles Thema, nämlich die Bedrohung der Unternehmen durch Wirtschaftskriminalität «von innen». Eine Vielzahl von Delikt- und Schadensfällen geht auf die Handlungen der eigenen Mitarbeiter zurück, ggf. im Zusammenspiel mit externen Dritten. Hier gilt es, die richtige Balance zu finden: Einerseits soll kein Klima des allgemeinen Misstrauens und Ausforschens entstehen, andererseits müssen aber auch klare Leitplanken gesetzt werden. Also: Eindeutigkeit bei den Regeln und Konsequenz bei der Sanktionierung von Verstössen.

Mit welchen Lösungen und Dienstleistungen können Sie Banken unterstützen?
Mit unserem Lösungsportfolio decken wir ein breites Spektrum an Compliance-Funktionalitäten ab. Es ist modular aufgebaut und wird von unseren Kunden ganz nach ihren Bedürfnissen eingesetzt. Wir bieten vorbereitete Module für die Bereiche Geldwäscherei, Insiderhandel und Marktmissbrauch, Namensabgleiche, Embargo-Überwachung und Interessenkonfliktmanagement an. Die Module umfassen jeweils eine Prüfkomponente zur Identifizierung von ungewöhnlichen oder risikoreichen Konstellationen und eine Fallbearbeitung zur

"Wenn mit technischer Unterstützung Risiken ermittelt werden, können mit denselben Methoden auch Chancen und Potenziale identifiziert werden."

Abklärung bzw. Entscheidung zu zuvor ermittelten Treffern und Dokumentationen.
Vor allem bieten wir den Instituten jedoch die Möglichkeit, Synergien aus der regulatorischen «Pflicht» für das operative Geschäft zu nutzen. Dazu bilden wir in unseren Lösungen bereits den Prozess der Kundenannahme ab, aus dem sich – neben vielen anderen Erfordernissen – auch eine Vielzahl von Compliance-Anforderungen ableiten lässt, sowohl im Hinblick auf die Risiken durch Geldwäscherei und Terrorismusfinanzierung als auch auf angrenzende Bereiche wie die «Tax Compliance». Für die Bank ergeben sich daraus gleich zwei entscheidende Vorteile: Zum einen kann das Client Onboarding mit grösster Effizienz erfolgen, trotz eventuell hoher Komplexität aufgrund eines umfangreichen Produktportfolios und internationaler Kundschaft mit jeweils unterschiedlichen Anforderungen an die erforderliche Dokumentation. Zum anderen steht im Ergebnis eine vollständige und qualitativ hochwertige Datenbasis zur Verfügung, die für die Betreuung des Kunden und den Ausbau der Geschäftsbeziehung genutzt werden kann. Neben unserer Rolle als Lösungsanbieter verstehen wir uns als universellen Umsetzungspartner, und wir stellen daher auch die erforderlichen Dienstleistungen in den Bereichen Projektmanagement, fachliche Begleitung und technische Beratung zur Verfügung.

Was sind Ihre wichtigsten Erkenntnisse aus bereits umgesetzten Projekten?
Technische Lösungen dürfen nicht zu kurz greifen. Bei IT-Anwendungen zur Sicherstellung der Compliance und Abwehr von kriminellen Handlungen liegt es in der Natur der Sache, dass sich die zugrunde liegenden fachlichen Definitionen im Laufe der Zeit verändern. Dies kann vielfältige Ursachen haben: Entweder gibt es neue Anforderungen seitens des Regulierers, es werden neue Erkenntnisse bezüglich abzuwehrender Tatmuster gewonnen oder aber die Bank kommt für sich selbst zu einer überarbeiteten Einschätzung von Risiken.

Das heisst: Die Regeln ändern sich. Und: Sie gehören in die Verantwortung der Fachexperten, nicht in die der IT.
Wir legen unsere Lösungen daher so aus, dass kein Bruch zwischen der fachlichen Definition von z.B. Monitoring-Szenarien oder Risiko-Modellen einerseits und deren technischer Umsetzung andererseits entstehen kann. Dazu setzen wir an den zentralen Stellen auf den Einsatz von grafischen Regelmodellen, die auch vollständig in die Hände der jeweiligen Experten, etwa aus den Bereichen Compliance, Legal oder Tax, gelegt werden können.

Auf den Punkt gebracht: Was gibt es aus Ihrer Sicht noch zu diesem Thema zu sagen? Was ist Ihr persönlicher Rat an das oberste Management?
Software-Lösungen alleine reichen nicht aus, um «compliant zu sein» und um Bedrohungen durch kriminelle Handlungen von aussen und von innen abzuwenden. Aber sie leisten einen wichtigen und unverzichtbaren Beitrag, zusammen mit organisatorischen Massnahmen und einer fortlaufenden Ausbildung und Sensibilisierung aller Mitarbeitenden.

Eine Gefahr besteht darin, technische Lösungen nur punktuell und als Reaktion auf aktuelle Anforderungen von aussen zu suchen. Oft werden dabei mögliche Synergien für das operative Geschäft übersehen oder zumindest nicht genutzt. Denn dort, wo es gilt, mit technischer Unterstützung Risiken zu ermitteln, können häufig mit denselben Methoden auch Chancen und Potenziale identifiziert werden, z.B. auf Basis von Informationen rund um den Kunden. Das ist die andere Seite von «Know your Customer».

ACTICO

EMEA
ACTICO GmbH
Ziegelei 5
88090 Immenstaad
Germany

info@actico.de
www.actico.de

Amerika
ACTICO Corp.
200 S. Wacker Dr.
Suite 3100
Chicago, IL 60606/USA

info@actico.com
www.actico.com

Asien & Pazifik
ACTICO Pte. Ltd.
11 Bishan Street 21
Singapore 573943

info@actico.com
www.actico.sg

02/2016

ACTICO ist ein führender international agierender Anbieter von Softwarelösungen und -technologien für das Decision Management.

In der digitalen Welt gilt es, riesige Datenvolumina zu verarbeiten und schnelle, konsistente und revisionssichere Entscheidungen zu treffen. Der Vorteil unserer Softwarelösungen: Geschäftsregeln und Prozesse lassen sich einfach anpassen und automatisiert ausführen. Das erhöht die Effizienz und Agilität unserer Kunden in ihrem Wettbewerbsumfeld. Damit können sie schneller wachsen, Innovationen effektiv auf den Markt bringen, compliant agieren und letztlich die Profitabilität steigern.

ACTICO bietet Softwarelösungen für die Bereiche:
- Kreditrisiko Management: Kreditrisiken bewerten und überwachen
- Kreditvergabe: Kreditprüfungen und -entscheidungen automatisieren
- Compliance: Transparenz ermöglichen, Regularien umsetzen, Betrug vermeiden
- Claims Management: Prozesse bei der Schadensabwicklung beschleunigen und konsistent und kostengünstig abwickeln
- Client Management: Vertrauliche Kundendaten sicher verarbeiten – vom Onboarding bis zum Reporting

Die Wurzeln von ACTICO gehen auf die 1997 gegründete Innovations Software Technology GmbH zurück, die 2008 Teil der Bosch-Gruppe wurde. Deren Softwaregeschäft für die Finanzbranche führt ACTICO seit November 2015 in einem eigenständigen Unternehmen weiter. Unsere inter-nationalen Kunden betreuen wir von unseren Standorten in Deutschland, USA und Singapur.

Mehr Informationen unter **www.actico.de**