ComplianceBusiness
Ausgabe 1 // März 2017

Digitalisierung im Compliancebereich

Mehr Daten, mehr IT – was muss die Compliance tun?

Von Bernd Michael Lindner und Uwe Bohle

Einleitung

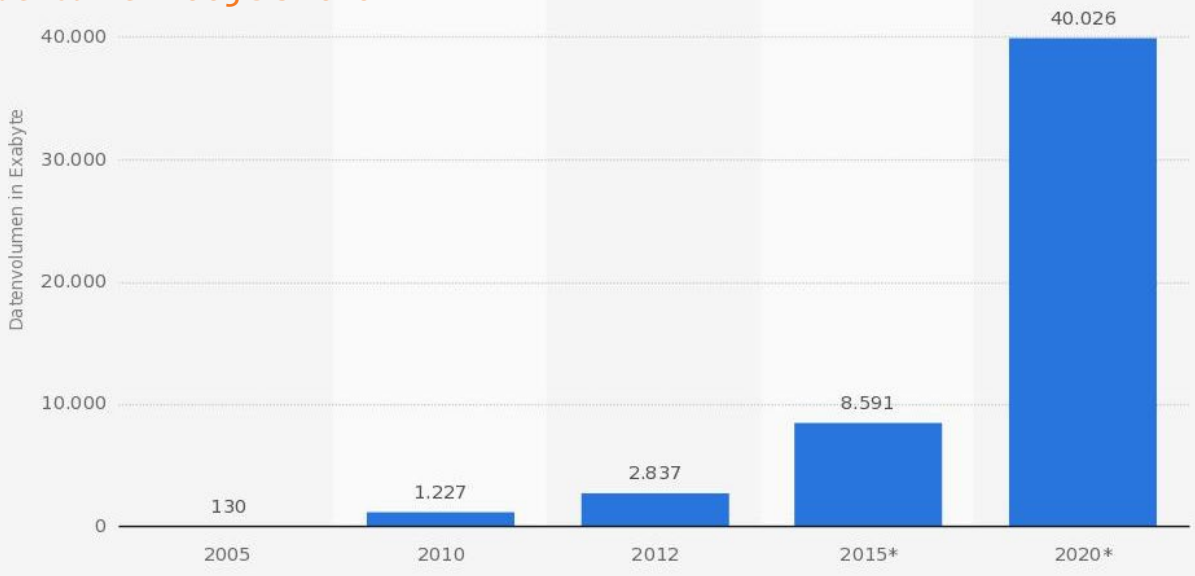
Die Nutzung digital vorhandener Daten nimmt durch die massenhafte Verbreitung von mobilen Endgeräten wie Smartphones, Tablets sowie Laptops und PCs ständig zu. Die Anzahl der Kunden, die zunehmend Finanzgeschäfte online durchführen, steigt. Eine Nutzung dieser steigenden Datenmengen ohne entsprechende IT-Systeme ist nicht mehr denkbar. Heute gibt es für sämtliche fachlichen und technischen Anforderungen entsprechende Softwarelösungen. Dies gilt auch für die IT-Ausstattung und Nutzung von Complianceeinheiten bei Finanzdienstleistern.

Die Compliance heute

Wer einen Blick in die Complianceeinheiten wirft, wird feststellen, dass neben den „klassischen" Frontend- und Backend-Systemen einer Bank zusätzlich weitere IT-Systeme in der Compliance zum Einsatz kommen, etwa für

- das Screening von Neu- und Bestandskunden sowie den Abgleich von Transaktionen gegen externe und interne Listen,
- das Geldwäschemonitoring,
- die Überwachung von Handels- und Mitarbeitergeschäften,

Prognose zum Volumen der jährlichen generierten digitalen Datenmenge weltweit in den Jahren 2003 bis 2020



Quelle:
IDC
© Statista 2017

Weitere Informationen:
Weltweit

ComplianceBusiness
Ausgabe 1 // März 2017

- die Erkennung von internem und externem Betrug,
- das Monitoring von neuen gesetzlichen und regulatorischen Anforderungen.

Genau in dieser Vielfalt von Systemen, Daten und Prozessen liegt eines der Hauptprobleme von Complianceeinheiten. Denn leider ist es oft so, dass benötigte Informationen aus mehreren Systemen zusammengestellt werden müssen, um dann in einem oft nur für diesen einen Fall erschaffenen Excel-Sheet zu landen. Beim Onboarding eines Kunden ist beispielsweise auffällig, dass Daten von einem System nicht automatisiert an ein anderes weitergegeben werden oder dass sogar noch Medienbrüche, verbunden mit der manuellen Erfassung von Daten, auftreten. Von einer durchgängigen IT-Unterstützung in den Complianceprozessen kann daher noch nicht gesprochen werden.

Ein weiteres Problem ist, dass der einzelne Mitarbeiter sicher in der Bedienung und der Nutzung dieser IT-Systeme sein muss. Ebenso wichtig ist das Wissen über die in diese Systeme einfließenden Daten oder die angeschlossenen Quellsysteme. Des Weiteren sind auch die Kenntnis der Prozesse, die diese Daten erzeugen, und der Zeitpunkt, zu dem diese Daten anfallen, von hoher Bedeutung.

All dieses Wissen hilft einem Compliancemitarbeiter, aus erzeugten Auffälligkeiten, Reports oder Meldungen die richtigen Schlüsse zu ziehen, effektiv und mit hoher Qualität eine Entscheidung zu treffen sowie die richtigen internen und externen Ansprechpartner einzubinden.

Zusammenfassend kann man festhalten, dass

- unterschiedliche Systeme zur Umsetzung der Complianceanforderungen genutzt werden,
- es keinen oder nur einen geringen Austausch von Daten zwischen den heterogenen Systemen gibt,
- Medienbrüche stattfinden,
- es keine durchgängige IT-Unterstützung in den Complianceprozessen gibt,
- Mitarbeiter oft nicht ausreichend geschult sind und wenige Kenntnisse über die Prozesse besitzen, die zu den Daten führen.

Aktuelles Thema „Digitalisierung“

Eine zusätzliche Herausforderung ergibt sich im Rahmen der sogenannten Digitalisierung. Hinter diesem inzwischen allgegenwärtigen Begriff verbergen sich auch Themen, die Compliance direkt und indirekt betreffen. Unternehmen eröffnen neue digitale Geschäftsmodelle und Vertriebswege, oft auch unter direkter Einbindung von neuen Marktbeteiligten wie Fintechs (Fintech ist eine Abkürzung für technologisch fortschrittliche Finanztechnologieunternehmen und setzt sich aus den Wörtern Financial Services und Technology zusammen).

Dafür gibt es bereits Beispiele:

- Die CreditPlus Bank, eine Tochter der Crédit Agricole, bietet einen Konsumentenkredit per iOS-App an, über den innerhalb von 15 Minuten entschieden wird.
- Die SolarisBank bietet über eine sogenannte API (Programmierschnittstelle) und das Portal AutoScout24 Sofortkredite an, über die innerhalber weniger Minuten entschieden wird.

Dadurch ändern sich für die betroffenen Organisationen die Wertschöpfungsketten und die Anforderungen an das bestehende Prozesstempo. Die durchgehende Datenverarbeitung vom Vertrieb bis zum Backoffice ist das Ziel. Ebenso nehmen in diesem Zusammenhang die Datenmengen, die zu einem Kunden gespeichert werden können, zu.

All diese Veränderungen wirken sich auch auf die Complianceeinheiten aus. Compliance muss die sich ändernden Geschäftsmodelle und Vertriebswege aktiv unterstützen und das zunehmende Prozesstempo mitgehen. Steigende Datenmengen und zunehmende Informationen über den Kunden müssen verarbeitet und interpretiert werden, um „Unterstützer“ und nicht „Verhinderer“ zu sein.

Die Herausforderungen für Compliance

Um diesen alten und neuen Herausforderungen effizient und effektiv begegnen zu können, sind Anpassungen dringend notwendig.

Die für Compliance relevanten Prozesse müssen durchgängig IT-gestützt sein, wobei sich die Anzahl der durch Compliance zu nutzenden Systeme auf einige wenige wichtige beschränken muss. Schnittstellen zwischen den IT-Systemen sind fachlich sinnvoll und technisch ein-

ComplianceBusiness
Ausgabe 1 // März 2017

wandfrei bereitzustellen, Datenverluste sind auf jeden Fall zu vermeiden. Dies gilt auch für Medienbrüche und die Notwendigkeit, Daten erneut zu erfassen, obwohl diese bereits vorhanden sind. Die Compliancesysteme selbst müssen auch Daten untereinander austauschen können, so muss der über ein Screeningtool ermittelte PeP-Status sowohl in das Geldwäschemonitoring als auch in die Risikoermittlung des Kunden einfließen – vollkommen automatisiert, ohne manuelle Erfassung in unterschiedlichen Systemen.

Ferner benötigt Compliance einen freien Zugang zu den relevanten Daten, um in Eigenverantwortung (ad hoc oder regelmäßig) Auswertungen durchführen zu können. Spontane Anfragen seitens des Vorstands oder des Wirtschaftsprüfers (etwa „Wie viele Geldwäscheverdachtsfälle pro Vertriebsregion gab es in den letzten drei Monaten, und wie viele davon führten zu einer Verdachtsmeldung?“) sind durch Compliance direkt zu beantworten. Dabei sollte es nicht so sein, dass eine solche Anfrage in einer Anforderung an die IT-Abteilung mündet, die dann nach einigen Tagen oder Wochen eine Auswertung liefert, die dann weitere Fragen aufwirft, welche dann nicht beantwortet werden können.

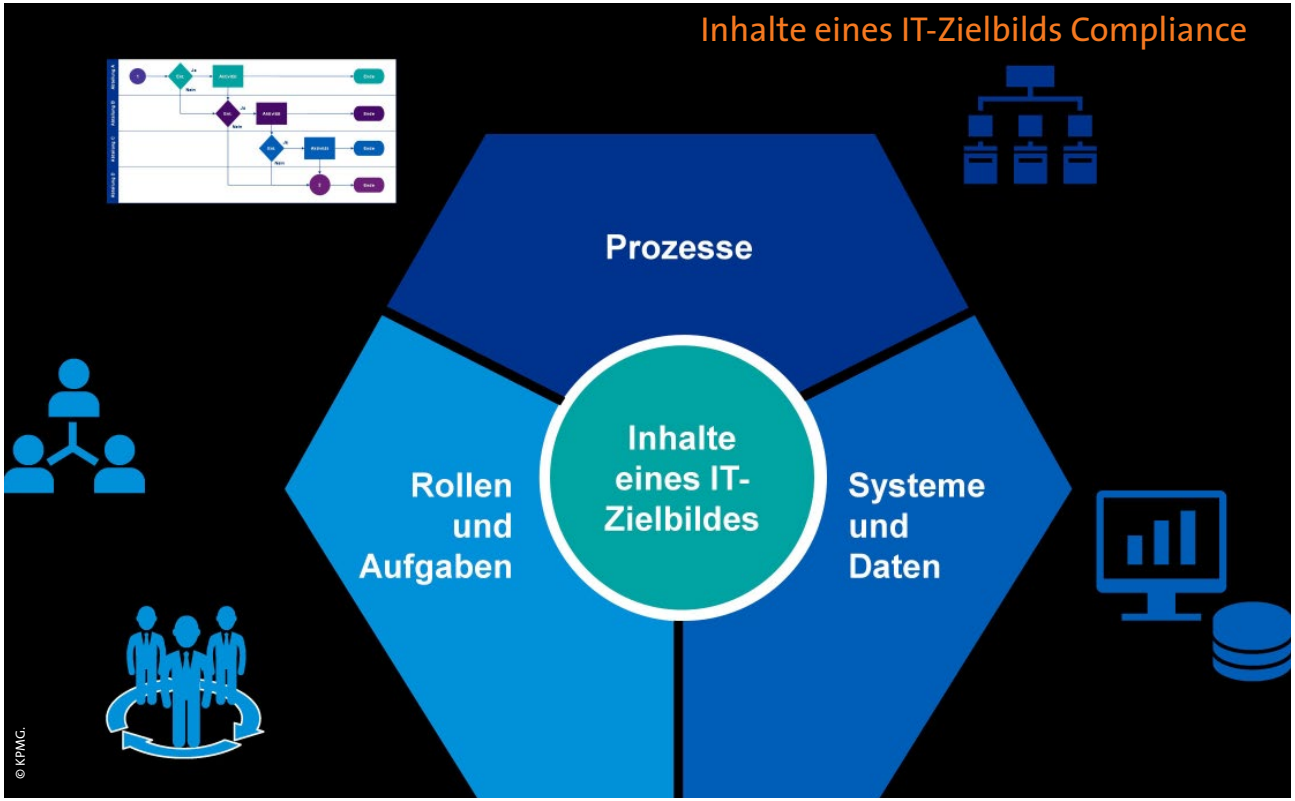
Ein wichtiger Aspekt im Zuge der IT-Unterstützung der Compliance ist eine regelmäßige und intensive Schulung der jeweils betroffenen Mitarbeiter in den IT-Systemen, die genutzt werden. Dies betrifft nicht nur die reine Bedienung der Systeme, sondern auch deren fachliche Administration, Parameter- und Regelpflege. Ein IT-System, das nicht richtig parametrisiert ist und dessen Benutzer die Funktionsweise des Systems nicht kennt, liefert auch keine brauchbaren Ergebnisse.

Ein möglicher Lösungsansatz

Wie kann Compliance es schaffen, den genannten Herausforderungen adäquat zu begegnen und Lösungen für diese zu entwickeln – und dies möglichst mit einem konkreten Aufwands- und Zeitplan?

Zunächst ist es wichtig, sich grundlegend Gedanken über ein IT-Zielbild für Compliance zu machen. Aber was ist eigentlich unter einem solchen IT-Zielbild zu verstehen, und welche Inhalte hat dieses IT-Zielbild?

Grundsätzlich ist im Rahmen des „IT-Zielbilds Compliance“ zu formulieren, welche betrieblichen Aufgaben und Prozesse durch Compliance unterstützt und welche dieser Aufgaben und Prozesse dabei IT-gestützt durchgeführt werden sollen. Dabei sind Verantwortlichkeiten und Rollen festzulegen.



ComplianceBusiness
Ausgabe 1 // März 2017

Das IT-Zielbild Compliance muss folgende Elemente berücksichtigen:

- Geschäftsstrategie des Unternehmens
- Geschäftsprozesse, Rollen und Aufgaben in diesen Geschäftsprozessen
- IT-Systeme und deren Schnittstellen
- Festlegung der Daten, die Compliance benötigt

Die Inhalte des IT-Zielbilds Compliance sind zu konkretisieren und mit den Fachbereichen, der IT und dem Vorstand abzustimmen.

Die Nutzenaspekte, die sich aus einem abgestimmten IT-Zielbild Compliance ergeben, sind unter anderem folgende:

- verbesserte Transparenz und Steuerbarkeit der IT-Ausrichtung der Compliance und eine klare Benennung der (strategischen) Ausrichtung
- ein konkret formuliertes Entwicklungsziel, das vom Management unterstützt und akzeptiert wird
- künftige Entwicklungen können auf Basis des IT-Zielbilds Compliance auf ihre Auswirkungen hin betrachtet werden
- Hebung von Synergien/Kostensenkungen, inkl. Investitionssicherheit

Nach Beschluss des IT-Zielbilds Compliance wird eine Ist-Analyse vorgenommen, um bestehende Abweichungen zwischen dem IT-Zielbild und dem Ist-Zustand festzustellen und entsprechend ihrer Bedeutung (etwa in Bezug auf das Risiko) auszuwerten. Daraus entwickelt sich ein genaues Bild der Handlungen, die zur Schließung der Gaps notwendig sind. Im Rahmen einer sich anschließenden Umsetzungsplanung wird dann eine entsprechende Zeit- und Aufwandsplanung erstellt.

Fazit

Ein IT-Zielbild Compliance beschreibt die IT-Ziele (Systeme, Daten, Prozesse), die zu erreichen sind, und schafft so die Voraussetzungen, diese IT-Ziele plan- und budgetierbar zu machen.

Gleichzeitig gibt es eine unternehmensweite Transparenz dieser IT-Ziele, und so kann auch Compliance seinen rechtmäßigen Platz in der IT-Strategie des Unternehmens finden und in den jährlich stattfindenden IT-Planungen berücksichtigt werden.

Bernd Michael Lindner,
Partner, KPMG,
Financial Services,
München

blindner@kpmg.com
www.kpmg.com

Uwe Bohle,
Senior Manager, KPMG,
Mannheim

ubohle@kpmg.com
www.kpmg.com