ComplianceBusiness
Ausgabe 1 // Juni 2015

Effektivität und Effizienz sind entscheidend

Für Unternehmen und IT-Dienstleister gilt: Beide Seiten sind gefordert

Von Uwe Bohle und Bernd Michael Lindner

In Zeiten der sich ständig erhöhenden gesetzlichen und regulatorischen Anforderungen (etwa: MaRisk, Solvency II, 4. EU-Geldwäscherichtlinie) ist die Ausübung der Compliancefunktion in einem Unternehmen ohne entsprechende Unterstützung durch Compliance-IT-Lösungen nicht mehr denkbar. Dabei ist nicht mehr nur die IT-Lösung selbst zu betrachten, sondern auch die im Unternehmen vorhandene Datenbasis, die zur Kontrolle und Überwachung heranzuziehen ist.

Diese IT-Lösungen sind in die Gesamtstrategie der Compliance einzubetten. Dabei gilt es, die Complianceteilrechtsgebiete sinnvoll IT-seitig zusammenzuführen und sich im Rahmen einer Compliance-IT-Strategie ein ganzheitliches Bild zu verschaffen, anstatt die Themen und IT-Lösungen isoliert voneinander zu betrachten.

Künftig führt dies zwangsläufig zu stärkeren Berührungspunkten zwischen Compliance- und IT-Einheiten, die Projekte und Aufgaben gemeinsam erfüllen müssen. In der Praxis stellen sich den beiden Einheiten übergreifende Fragen:

„Wir haben zu viele „false positives" in unserer Liste, wie sollen wir das zeitnah bearbeiten?"

„Die Dateneinspielung in der letzten Nacht ist nicht durchgelaufen, wir haben kein aktuelles Monitoring!"

„Nach dem Softwareupdate hat sich die Laufzeit der Prüfung derart erhöht, dass die Nachtverarbeitung jetzt bis morgens um 10:00 andauert!"

Solche und ähnliche Aussagen sind durchaus keine Seltenheit in Complianceeinheiten, die IT-Systeme in ihrer täglichen Arbeit einsetzen.

Die Wahrnehmung der ständig steigenden Complianceaufgaben kann heute nur noch mit der Unterstützung von Spezialsoftware erfolgen. Millionen von Datensätzen müssen regelmäßig auf compliancerelevante Sachverhalte hin überprüft werden. Sei es die Überwachung von Geschäfts- und Transaktionsdaten oder die Kontrolle von Bestandsdaten – ohne effektive Softwarelösungen ist dies nicht mehr möglich.

Effizientes Datenmanagement lebt vom guten Zusammenspiel von Unternehmen und IT-Dienstleistern.

Dabei sind, neben der Erfüllung fachlicher Anforderungen, viele weitere IT-Themen zu beachten, die sich

ComplianceBusiness
Ausgabe 1 // Juni 2015

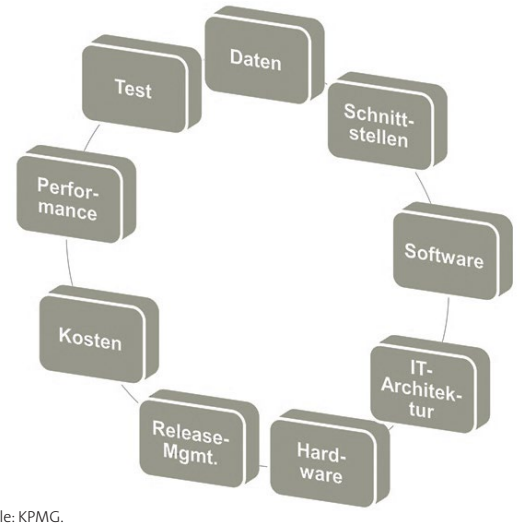
direkt oder indirekt auf die Effizienz einer Complianceeinheit auswirken.

Gestiegene Anforderungen an Daten und Software

In den vergangenen Jahren haben sich die Complianceeinheiten sukzessive IT-Lösungen beschafft, um den ständig steigenden Anforderungen an Kontrollen und Überwachungen gerecht zu werden. So hat sich nach und nach eine Softwarelandschaft gebildet, deren Bestandteile in den seltensten Fällen aus einer Hand stammen und kompatibel zueinander sind.

Zusätzlich haben sich die Anforderungen an die zu prüfenden Datenfelder stetig erhöht. Kundenkonten und -daten sind jedoch oft schon viele Jahre im Bestand. Eine ständige Anpassung aller Daten mit entsprechendem Nachbearbeitungsaufwand konnte da oftmals nicht erfolgen. Des Weiteren sind durchgeführte Systemmigrationen oder Fusionen in vielen Fällen weitere Quellen von unvollständigen oder gar falsch gefüllten Datenfeldern.

So stellt sich heute für einen Chief Compliance Officer (CCO) und seine Mitarbeiter häufig nicht nur die Frage nach der Aktualität der genutzten Compliancesoftware, sondern auch die nach der Qualität der aus den Systemen bereitgestellten Daten. Ein IT-System kann noch so aktuell und gut parametrisiert sein – Datenmängel können so nicht beseitigt werden. Das führt etwa zu einer großen Anzahl von sogenannten „false positives“, also angeblichen Treffern, die sich als nicht relevant herausstellen. Doch auch nicht relevante Treffer müssen durch die Compliancefunktion bearbeitet und als solche gekennzeichnet werden. Dies bindet oft unnötig Kapazitäten und hindert die Mitarbeiter an der Wahrnehmung ihrer eigentlichen Complianceaufgaben.



Quelle: KPMG.

Trifft das Datenqualitätsproblem zudem auf nicht aktuelle Software oder eine nicht aktuelle Parametrisierung, kann sich dieser „Zustand“ noch verschlimmern.

Performance

Ein weiteres IT-Thema, das die Ressourcen der Compliancefunktion massiv beansprucht, sind zu lange Wartezeiten bei der Dateneinspielung oder Datenverarbeitung. Bestandsdaten müssen regelmäßig mit Embargo-, Sanktions- und PeP(politisch exponierte Person)-Listen abgeglichen werden. Werden die Listen aktualisiert, sind alle Bestandsdaten erneut gegen diese Listen zu prüfen. Das erfordert ein effektives und zeitnahes Listenmanagement (fachlich wie technisch). Aber auch die der Software zugrundeliegende IT-Infrastruktur muss mitspielen. Zu geringe Hauptspeicherkapazitäten, zu wenig Prozessorleistung oder nicht ausreichender Festplattenspeicher können leicht zu Verarbeitungszeiten von mehr als zwölf Stunden führen. Das wiederum kann leicht zu Verspätungen am Tagesstart führen, so dass Compliancesysteme etwa für Onlineanfragen im KYC-Prozess nicht bereitstehen.

Im Rahmen der Transaktionsprüfung ist das Thema Performance noch stärker zu gewichten. Hier wird Transaktion sehr weit am Ende des Zahlungsverkehrsprozesses geprüft. Insofern darf die Weitergabe von Zahlungen nicht wesentlich verzögert werden, um z.B. bestehende Cut-off-Zeiten einzuhalten.

Einbindung in die IT-Architektur

Heute ist es für Compliance und desgleichen für die betroffenen Fachbereiche unerlässlich, Erkenntnisse aus IT-gestützten Monitoring- und Screeningprozessen auch in den Bestandssystemen zu hinterlegen – sei es der ermittelte Risikograd des Kunden im Rahmen der einzuhaltenden Sorgfaltspflichten oder die Erkenntnis, dass es sich bei dem Kunden um eine politisch exponierte Person (PeP) handelt. Oftmals sind die Compliance-IT-Systeme ausschließlich über Datenlieferungen als Datei „angebunden“, so dass eine IT-basierte Rückmeldung der Compliancesoftware in die Konzernwelt zurück nicht oder nur sehr aufwendig möglich ist. Hier muss oft-

ComplianceBusiness
Ausgabe 1 // Juni 2015

mals auf manuelle Prozesse zurückgegriffen werden. Diese sind fehleranfällig, bedürfen der Kontrolle und Überwachung sowie finden zeitverzögert gegenüber einer IT-Lösung statt.

Hier ist es wichtig, die wesentlichen beteiligten Bestands- und Compliancesysteme zu identifizieren und Maßnahmen zu ergreifen, um einen IT-gestützten Austausch von Informationen zu gewährleisten.

Kosten

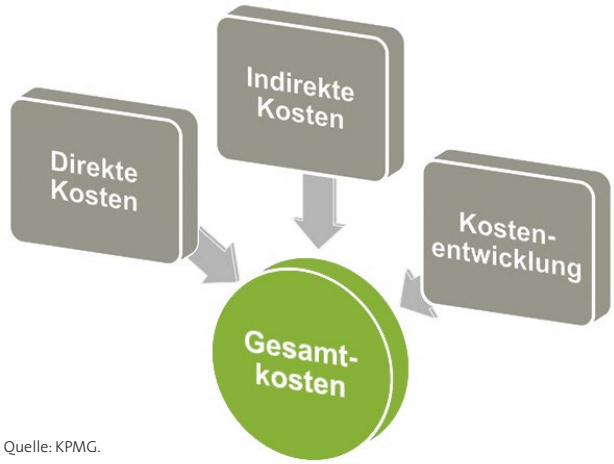
In Zeiten steigenden Kostendrucks sind auch Complianceeinheiten angesprochen, wenn es um Kostenreduzierung geht. Compliance-IT-Systeme sind mitunter wahre Datensenken, die (fachlich sinnvoll oder nicht) möglichst viele Daten aus unterschiedlichen Systemen sammeln und für viele Jahre aufbewahren, etwa zur Bildung von statistischen Auswertungen. Auch wenn in den vergangenen Jahren die Kosten für das Speichern von Daten ständig zurückgegangen sind, entpuppt sich manche Compliance-IT-Landschaft als eine immense Kostenposition. Dabei ist es durchaus sinnvoll, einen gesamthaften Blick auf direkte und indirekte Kosten der eingesetzten Compliance-IT-Landschaft zu werfen und diese auch im Hinblick auf die zukünftige Entwicklung wie Anzahl der User, Mengenwachstum der Datenbanken, Archivierung und Datensicherung zu beurteilen. Nicht zu vergessen sind Kosten für Lizenzen und Wartung, Release- und Upgradekosten sowie laufende Kosten im Rahmen von internen Weiterentwicklungen (Schnittstellen, Reports, etc.).

Softwaretest

Ein immer wieder auftretendes Problem im Zusammenhang mit Compliance-IT-Lösungen ist die Durchführung von korrekten und vollständigen Tests im Rahmen von Releases oder der Umsetzung von Anforderungen. Die Complianceeinheit muss sicherstellen, dass nach einem Release keine unerwarteten Treffer oder Monitoringergebnisse entstehen. Die korrekte Auslieferung von Software ist sicherlich zuerst Aufgabe des Softwareherstellers. Jedoch sind im Rahmen der Einführung von Standardsoftware in der Regel kundenindividuelle Anpassungen (Customizing) vorzunehmen. Des Weiteren ist die Parametrisierung des Systems eine höchst individuelle Einstellung und auf die jeweiligen Bedürfnisse des Konzerns zugeschnitten.

Damit ist es für Compliance unerlässlich, fest definierte Testfälle und Testdaten zu besitzen, die im Falle eines noch so kleinen Patches oder Releases effizient durchlaufen können. Die Vergleichbarkeit der Ergebnisse „vor Release“ und „nach Release“ schafft Sicherheit in Bezug auf die Ergebnisse der IT-Lösung. Gleichzeitig können dadurch recht schnell eine fehlerhafte Releaseauslieferung des Herstellers festgestellt und die Aufwände in Compliance und der IT reduziert werden. Dieses Vorgehen setzt selbstverständlich eine saubere Trennung von Entwicklungs-, Test- und Abnahmeumgebungen voraus.

Die Bereitstellung oder Nutzung von qualitativ hochwertigen Testdaten ist ein weiteres Thema im Zusammenhang mit dem Test von Software. Oftmals werden Echtdaten benötigt, um etwa die Parametrisierung eines Tools im Finanzsanktions- und Embargoumfeld korrekt vorzunehmen. Stehen diese Daten z.B. aus Datenschutzgründen nicht zur Verfügung, müssen qualitativ hochwertige künstliche Testdaten selbst erstellt werden.

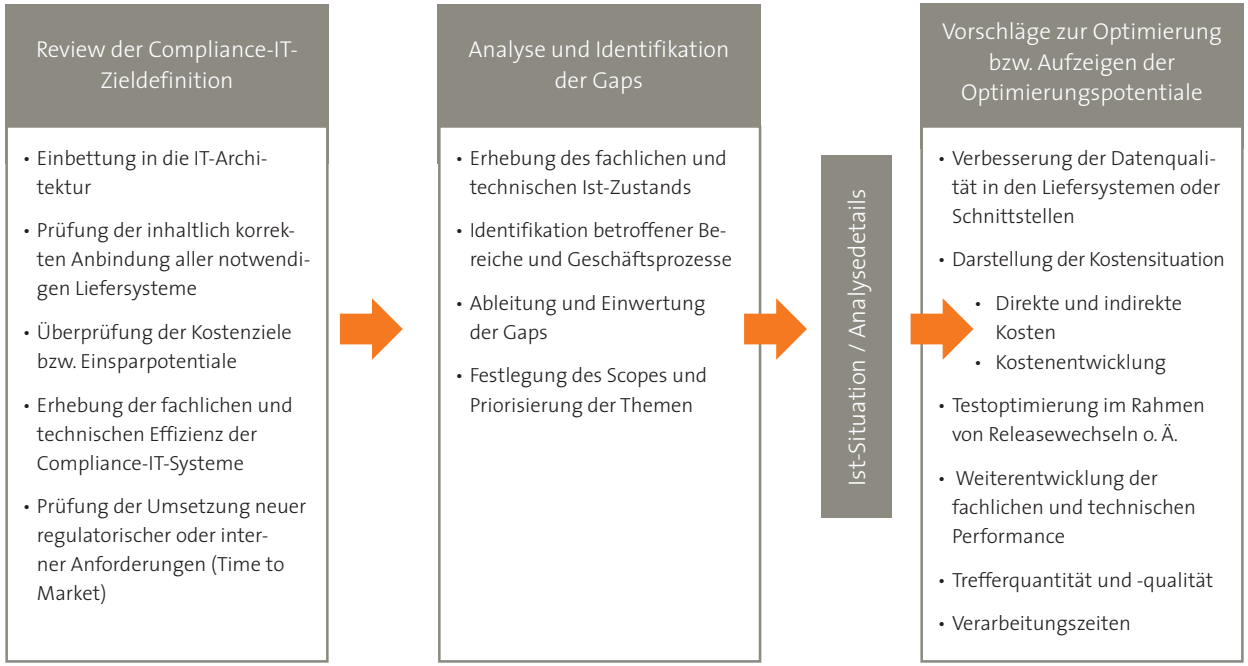


Quelle: KPMG.

Fazit

Aufgrund der inzwischen starken Einbindung der Complianceeinheiten in die Konzerne und deren starker Nutzung von Compliancespezialsoftware ist es heute zwingend notwendig, IT-Systeme und Prozesse effektiv aufzusetzen und dabei Kosten, fachliche und technische Effizienz der Lösungen nicht aus den Augen zu verlieren.

ComplianceBusiness
Ausgabe 1 // Juni 2015



Eine Compliance-IT-Gap-Analyse ermöglicht die Identifikation aktueller Handlungsfelder und die risikobasierte Priorisierung im Rahmen der Optimierungspotentiale.

Quelle: KPMG.

Lösungsansatz in der Praxis

In einem ersten Schritt werden die festgelegten Ziele einer Compliance-IT-Strategie überprüft und gegebenenfalls überarbeitet oder angepasst. Dies muss in engem Austausch mit der IT-Abteilung erfolgen und sollte fachliche und technische Aspekte gleichermaßen berücksichtigen. Auf Basis der Zieldefinition erfolgen eine Analyse des aktuellen Stands und ein Abgleich mit dem Compliance-IT-Zielbild. Mit Hilfe der Analyseergebnisse werden Optimierungspotentiale aufgezeigt und konkrete Vorschläge zur Optimierung erarbeitet.

Uwe Bohle,
Consulting Financial Services, Senior Manager,
KPMG, Mannheim
ubohle@kpmg.com
www.kpmg.com

Bernd Michael Lindner,
Partner, Financial Services
KPMG, München
blindner@kpmg.com
www.kpmg.com