www.boersen-zeitung.de

Börsen-Zeitung SPEZIAL

Verlagsbeilage zur Börsen-Zeitung | 6. März 2014 | Nr. 45

Creative Power

Für unsere anspruchsvollen Kunden realisieren wir Medien in Print, Online und Mobile. Unsere Redakteure, Grafiker und Kommunikationsfachleute machen bereits heute über 4.000 Redaktionsseiten für unsere Kunden bzw. Mandanten.

Wir beraten Sie gerne professionell und persönlich, wenn es um Ihre Kundenmedien geht.

Ihr Corporate-Media-Partner

Keppler Medien Frankfurt GmbH
Geschäftsleitung
Postanschrift: Industriestraße 2, 63150 Heusenstamm
Telefon: 06104 / 606 – 133, Telefax: 06104 / 606 – 117
E-Mail.: phr(at)kepplermediengruppe.de
www.kepplermediengruppe.de

Keppler Medien Gruppe

FORUM CORPORATE PUBLISHING

Inhalt

Impressum

Redaktion: Claudia Weippert-Stemmer
Anzeigen: Dr. Jens Zinke (verantwortlich) und Stephan Sandner
Technik: Tom Maier
Gestaltung und typografische Umsetzung: Bernd Handreke

Fotos: fotolia

Druck: Westdeutsche Verlags- und Druckerei GmbH, Kurhessenstraße 4–6, 64546 Mörfelden-Walldorf

Verlag Börsen-Zeitung in der Herausgebergemeinschaft WERTPAPIER-MITTEILUNGEN Keppler, Lehmann GmbH & Co. KG, Düsseldorfer Straße 16, 60329 Frankfurt am Main
Tel.: 069/27 32-0
Anzeigen Tel.: 069/27 32-115, Fax: 069/23 37 02
Vertrieb Fax: 069/23 41 73
Geschäftsführung: Ernst Padberg, Markus Heer (stv.)

Compliance Management jenseits der eigenen vier Wände

Gesamte Lieferkette muss ökologische, ethische und arbeitsrechtliche Standards befolgen

Jürgen Kunz
Partner
KPMG AG
Wirtschaftsprüfungsgesellschaft

Sven T. Marlinghaus
Partner und Head of
Strategy & Operations
Consulting Germany
KPMG AG
Wirtschaftsprüfungsgesellschaft

Das Prinzip der Zurechnung, bei dem ein Unternehmen für Verstöße seiner Zulieferer haftet, setzt sich weltweit immer stärker durch. International stehen dafür Regelungen wie das Antikorruptionsgesetz UK Bribery Act oder der US-amerikanische Dodd-Frank Act. Auch Änderungen des Deutschen Corporate Governance Kodex oder auch neue und veränderte branchenspezifische Gesetze und Kodizes lassen ähnliche Entwicklungen erwarten.

Gleichzeitig steigt auch der öffentliche Druck auf die Unternehmen: Zu Recht wird erwartet, dass nicht nur in den eigenen vier Wänden rechtskonform und nachhaltig gehandelt wird, sondern auch, dass in der gesamten Lieferkette ökologische, ethische und arbeitsrechtliche Standards eingehalten werden. Vor diesem Hintergrund richtet auch die Financial Community ihren Blick verstärkt auf die Effizienz und Effektivität der auf die Lieferketten ausgerichteten Kontrollmechanismen – die jedoch häufig erhebliche Schwächen aufweisen.

In vielen Unternehmen sind die für das Compliance Management der Supply Chain notwendigen Methoden und Lösungsansätze prinzipiell vorhanden. Dabei sind jedoch die Gesamtsysteme fast immer sehr stark auf das eigene Unternehmen zugeschnitten: Im Hinblick auf die Sicherstellung der Transparenz und Compliance innerhalb des Zuliefernetzwerks existieren teilweise eklatante Schwachstellen. Ein Kernproblem ist dabei die fehlende institutionalisierte Zusammenarbeit zwischen der Finanzabteilung auf der einen und der Einkaufsabteilung auf der anderen Seite. Zwar verfügen die Finanz- und Risikoexperten über die für das Compliance Management notwendigen Instrumente. Ihnen fehlt jedoch der tiefe Einblick des Einkaufs und der Logistik in das externe Wertschöpfungsnetzwerk und damit in der Regel auch das Wissen um das konkrete Anwendungsszenario.

Teilweise eklatante Schwachstellen

Der abteilungs- und standortübergreifenden Vernetzung der Kompetenzen kommt deshalb im Hinblick auf die Compliance-Strategie eine kritische Bedeutung zu. Sind alle Beschaffungsprozesse transparent gestaltet? Bestehen verbindliche Vorgaben zur Lieferantenauswahl? Entsprechen Musterverträge aktuellen rechtlichen Vorgaben? Existieren Standardprozesse zur Auftragsvergabe, Kontrolle von Rechnungen und zur Freigabe von Zahlungen? Das sind Fragen, die nur aus der Kooperation der Finanz- und Einkaufsabteilungen heraus beantwortet werden können.

Ein Code of Conduct für Zulieferer, der rechtliche Risiken mit Geschäftspartnern verhindert und Standards entlang der gesamten Lieferkette schafft, ist dabei ein zentrales Instrument. Darin sollten alle wichtigen Klauseln, beispielsweise zur Vermeidung von Kinderarbeit oder zum Umweltschutz enthalten sein, zu deren Einhaltung sich die Lieferanten vertraglich verpflichten. Zudem sollte ein solches Regelwerk Maßgaben zur Selbstüberprüfung des Lieferanten zur Einhaltung der Klauseln einfordern. Da Papier jedoch bekanntlich geduldig ist, sollte dem Kunden die Möglichkeit zur Verfügung stehen, die Einhaltung der Vorgaben überprüfen und bei Verstößen Kündigungsrechte und Sanktionen geltend machen zu können. Haben beide Parteien eigene, nicht voll kompatible Compliance-Kodizes, sind Konflikte vorprogrammiert.

Diese lassen sich allerdings lösen, oder von vornherein vermeiden, etwa mit den vom BDI oder BME entwickelten Formulierungshilfen für eine gegenseitige Anerkennung von Verhaltenskodizes. Im Vordergrund steht dabei zwingend die partnerschaftliche Beziehung zum Lieferanten: Entsteht der Eindruck, dass Überprüfungen vor allem dem Ausspähen von sensiblen Informationen dienen, ist der Vertrauensschaden enorm. Eine intensive präventive und begleitende Kommunikation und hohe Transparenz sind deshalb erfolgskritisch.

Um den entstandenen Verpflichtungen und Risiken in der Wertschöpfungskette gerecht zu werden, bedarf es entsprechender Organisationsstrukturen und Maßnahmen. Durch ein wirksames Compliance-Management-System (CMS) wird den Anforderungen Rech-

nung getragen. Es identifiziert neue Risiken aus aufgedeckten Schwachstellen und überwacht bzw. verbessert permanent alle Compliance-Maßnahmen. Die Ziele eines CMS sollten folgende sein:

- **Orientierungs-, Sicherheits- und Beratungsfunktion –** Klare Strukturen und Prozesse schaffen, die das rechts- und regelkonforme Verhalten aller Mitarbeiter fördern und ermöglichen; insbesondere Sicherheit in einem immer komplexeren Regelungsumfeld erzeugen.
- **Proaktive Risikosteuerung –** Erkennen, Managen und Überwachen von Compliance-Risiken; insbesondere Compliance-Verstöße aufdecken und vorab definierte Maßnahmen nachverfolgen.
- **Schutzfunktion –** Folgen von Non-Compliance für Unternehmen und Organe reduzieren und vermeiden, insbesondere wirtschaftlich schädigende Handlungen, zivil- und strafrechtliche Konsequenzen, finanzielle Schäden und Reputationsschäden.
- **Effizienzsteigerung –** Bereits bestehende Compliance-„Inseln" identifizieren und koordinieren.
- **Reputationsfunktion –** Compliance Management kann das Vertrauen der Geschäftspartner, der Öffentlichkeit und sonstiger Stakeholder sichern.

Die Maßnahmen des Compliance-Programms dienen sowohl der Prävention als auch zur Aufdeckung von Fehlverhalten und Schwachstellen. Sie sind auf die Verhinderung von Regelverstößen gerichtet und erkennen etwa durch Einrichten eines Hinweisgeberverfahrens potenzielle Compliance-Verstöße und reagieren auf erkannte Risiken und Verstöße. Darüber hinaus kann ein wirksames Compliance-Programm zu einer adäquaten Kommunikation an die zuständigen internen und externen Stellen beitragen und eine Ursachenanalyse ermöglichen.

Ein zukunftsweisendes und Sicherheit bietendes Compliance-System ist jedoch nicht allein darauf ausgelegt, Anforderungen und Regularien zu verschriftlichen: Denn einerseits geht es darum, unternehmens- und abteilungsübergreifende Prozesse und Strukturen zu etablieren und ein gemeinsames Verständnis für das Thema zu entwickeln. Dabei sind auch der Einsatz übergeordneter IT-gestützter Compliance Tools und die Zentralisierung des Compliance Management der Tochtergesellschaften von großer Relevanz.

Andererseits muss sichergestellt werden, dass die eigenen Sorgfaltspflichten im Hinblick auf die Compliance des Zuliefernetzwerks voll erfüllt sind,

Von Compliance zu Performance

wofür die Unterschrift des Zulieferers unter entsprechenden Vereinbarungen und Dokumenten nicht ausreichend ist. Eine nachhaltige Lösung bietet eine umfassende und testierte Prüfung des Compliance-Management-Systems des Zulieferers durch externe Experten. Hierfür bietet beispielsweise der 2011 vom Institut der Wirtschaftsprüfer veröffentlichte branchenunabhängige Prüfungsstandard (PS) 980 die Grundlage, indem er die Bestandteile eines CMS sowie ein Rahmenwerk für dessen Prüfung definiert.

Die kritische Rolle eines die gesamte Wertschöpfungskette fokussierenden Compliance Management hat auch Implikationen für das übergeordnete Performance Management des Unternehmens und insbesondere für die Gestaltung globaler Wertschöpfungsnetzwerke: So werden etwa die Kosten für das Compliance Monitoring und die zunehmenden Auswirkungen von Compliance-Risiken zu wesentlichen Faktoren bei einer Total-Cost-Betrachtung des Supplier Network. Die Entwicklung und Implementierung integrierter Performance-Management-Systeme, die alle aus der Compliance-Perspektive relevanten Faktoren berücksichtigen, werden deshalb in den kommenden Jahren zu den wichtigsten Aufgaben der Einkaufs- und Supply-Chain-Management-Abteilungen gehören.

Effizienz trotz Vielfalt – nur mit Standards möglich!

Zuversichtlich für Asset-Management-Branche – Logistikunternehmen machen es vor

Dr. Stephan Meisenzahl
Business Consultant
concedro GmbH

Dr. Thomas Redelberger
Securities Initiatives
SWIFT

Heute bestellt – morgen geliefert. Dank konsequenter Automatisierung und Standardisierung in den Bestell- und Abwicklungsprozessen vollzog sich in den letzten Jahren ein radikaler Wandel im Online-Handel. Online-Händler sind aktuell in der Lage, trotz hoch komplexer Vorgänge Bestellungen bereits am Folgetag zu liefern. Hierzu ist es nicht ausreichend, nur die internen Prozesse im Griff zu haben. Es existiert eine fragmentierte Landschaft aus vielen kleinen unabhängigen Verkäufern sowie Produzenten und Logistikunternehmen, die der Online-Händler in die eigenen Abläufe integriert.

Ähnlich hohe Komplexität bezüglich der Kommunikation in den Abwicklungsprozessen entstand in den vergangenen Jahren im Asset Management. Mit der Einführung des vierten Finanzmarktförderungsgesetzes 2002 schaffte der deutsche Gesetzgeber die Grundlage für ein weitreichendes Outsourcing und damit für eine Spezialisierung in der Branche. Seitdem brechen die Wertschöpfungsketten sukzessive auf und verteilen sich zunehmend auf verschiedene Häuser. Selbst Kerntätigkeiten, wie das Portfoliomanagement, werden verstärkt von externen Spezialisten erbracht. Beispielsweise stieg die Anzahl der externen Portfoliomanager, die per SWIFT an eine Kapitalverwaltungsgesellschaft (KVG) angebunden sind, von 53 im Jahr 2006 auf 130 im Jahr 2013.

Neben der klassischen KVG, die weitestgehend alle relevanten Leistungen selbst erbringt, etablierten sich zwei weitere Spezialisierungen in den Geschäftsmodellen: das Beratungs- und das Verwaltungsmandat. Im Beratungsmandat unterbreitet ein externer Anlageberater der KVG eine Anlageempfehlung. Die Prüfung der Anlagegrenzen und die finale Umsetzung erfolgen in eigener Verantwortung durch das KVG-eigene Portfoliomanagement. Im Verwaltungsmandat hingegen trifft der externe Portfoliomanager die tatsächliche Anlageentscheidung. Die KVG prüft ex post die Einhaltung der Anlagegrenzen.

Die zunehmende Vergabe von Tätigkeiten der KVG an externe Spezialisten führt zu einer Vervielfachung der Kommunikationsbeziehungen. Dies hat der Bundesverband Investment und Asset Management (BVI) im Rahmen der Wertpapiertransaktionsstandards 2004 frühzeitig thematisiert. Ziel war die Entwicklung einer deutschen Market Practice, die die idealtypischen Geschäftsabläufe und die externe Kommunikation mit den Geschäftspartnern aufzeigt.

Heute bestellt, morgen geliefert?

Trifft das Motto aus der Logistikbranche, heute bestellt – morgen geliefert, auch im Asset Management zu? Wie gut sind die internen Abläufe nach der Standardisierungsinitiative mit den externen Prozesspartnern heute abgestimmt? concedro führte zur Untersuchung dieser Fragen im Zeitraum Oktober 2013 bis Januar 2014 eine Studie im Advisory-Umfeld mit dem Fokus auf die Standardisierung in den Abwicklungsprozessen durch. Hierzu wurden KVGen, Master-KVGen, Depotbanken und Global Custodians befragt.

Danach beurteilen lediglich ein Viertel der Studienteilnehmer die Zusammenarbeit im Advisory als weitestgehend standardisiert. Mehr als 60% bewerten die Prozesse mit ihren Geschäftspartnern als nur teilweise standardisiert. Knapp 10% schätzen diese sogar als „weitestgehend individuell“ ein.

Eine eindeutige Verantwortlichkeit der Beteiligten für die Lieferinstruktion (SSI) der Wertpapiergeschäfte und die Wahl der Lagerstellen ist aufgrund unterschiedlicher Angaben der teilnehmenden Häuser nicht erkennbar.

- Die Mehrheit der KVGen sieht bei der Angabe der Lagerstelle das

KVG-eigene oder das externe Portfoliomanagement in der Pflicht. Demgegenüber sehen sich eine Vielzahl der Depotbanken/Custodians hierfür selbst in der Verantwortung.

- Drei Viertel der KVGen halten sich oder den Portfoliomanager für die Einholung der Lieferinstruktion verantwortlich und zu einem Viertel den Broker. Dagegen erachten sich diesbezüglich die Depotbanken/Custodians zu einem Viertel auch für zuständig.
- Für die Klärung von Unstimmigkeiten in den Abwicklungsinstruktionen scheint es keine klaren Zuständigkeiten zu geben. Von den Studienteilnehmern werden alle Beteiligten der Prozesskette als verantwortlich genannt.

Potenzial zur Standardisierung zeigt sich auch bei den im Advisory-Umfeld eingesetzten Kommunikationsmitteln. Gemäß den Umfrageergebnissen wird SWIFT im Vergleich zu Omgeo deutlich stärker in der Kommunikation verwendet. Dennoch kann bei einem Anteil von zwei Dritteln bei klassischen Wertpapieren und etwas mehr als der Hälfte bei Devisengeschäften nicht von einem einheitlichen Kommunikationsstandard gesprochen werden. Weniger standardisierte Formate, wie Fax und E-Mail, besitzen mit einem Fünftel bei klassischen Wertpapieren und einem Drittel bei Devisen noch immer einen substanziellen Anteil an der Kommunikation.

Selbst im Einsatz von SWIFT, das eine hohe Standardisierung zum Ziel hat, lassen sich unterschiedliche Handhabungsweisen in der Nutzung der optionalen Felder feststellen. Bei zentralen Nachrichtentypen, wie der Brokerabrechnung (MT515) oder den Lieferinstruktionen (SSIs) an die Depotbank (MT541/543), sind bei den befragten Teilnehmern kaum einheitliche Verwendungsmuster erkennbar, obgleich hierfür dokumentierte SMPG-Standards zur Verfügung stehen.

Trotz der genannten BVI-Initiative im Jahr 2004 stellt sich heraus, dass Prozessdetails und Verantwortlichkeiten nach wie vor unterschiedlich gehandhabt werden. Ineffizienzen und zusätzliche Komplexität in den Abläufen der einzelnen Beteiligten sind die Folge.

„Der BVI fördert Effizienz und Erfolg seiner Mitglieder. Der Verband unterstützt eine weitergehende Standardisierung der Kommunikationsprozesse in der Branche. Der BVI mit seiner zehnjährigen Erfahrung in Wertpapiertransaktionsstandards für KVGen ist die ideale Plattform für eine solche Initiative."

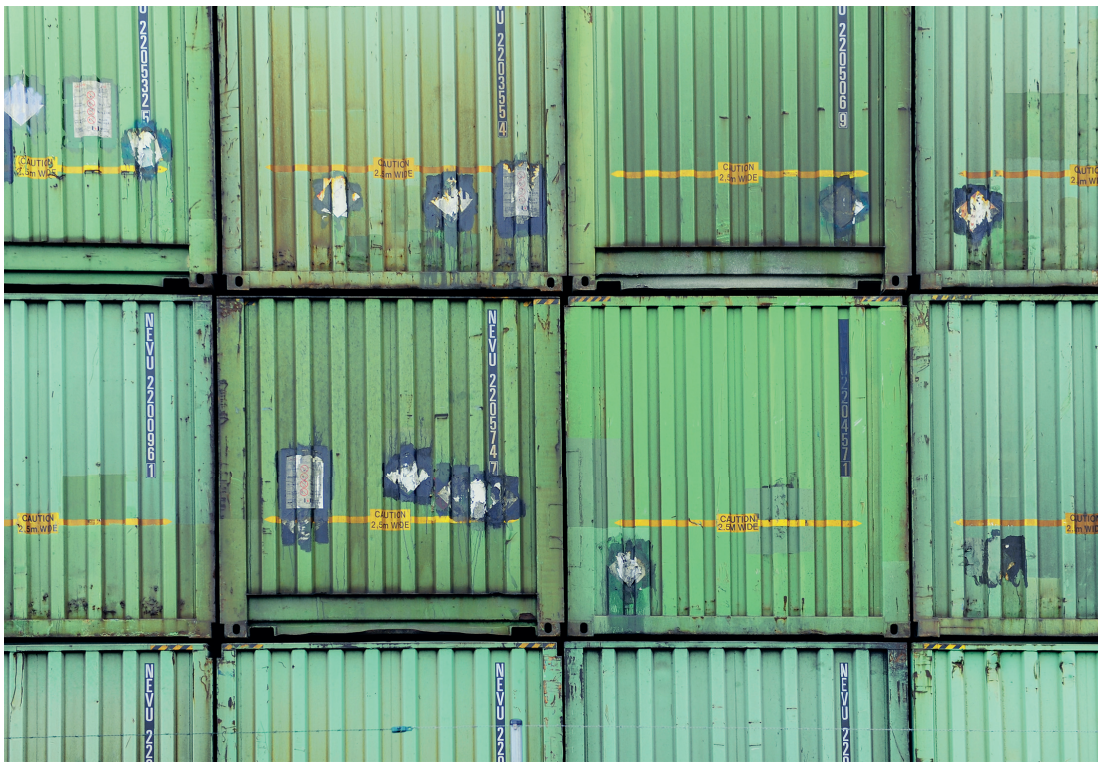
Rudolf Siebel, Geschäftsführer BVI

Ungeachtet eines weitergehenden Standardisierungsbedarfs in den Häusern bietet SWIFT auf operationeller und technischer Ebene eine Möglichkeit zu einer hohen Standardisierung. Mit den Geschäftspartnern sind nur minimale Absprachen notwendig, da Sicherheitsmechanismen und technische Verbindungsdetails weltweit einheitlich sind. Die Kosten für die Einrichtung und den Betrieb eines SWIFT-Anschlusses sind über die Jahre stetig gefallen, auch dank einer Cloud-Anbindung (SWIFT Lite2), die in den SWIFT-Rechenzentren in den Niederlanden und der Schweiz betrieben wird.

Vor dem Hintergrund des Kostentreibers Prozessheterogenität ist es wenig überraschend, dass eine weitergehende Standardisierung bei fast 90% der Studienteilnehmer eine hohe bis sehr hohe Relevanz hat. In Zusammenarbeit mit den jeweiligen Verbänden, BVI bei KVGen und Bankenverband bei Depotbanken bzw. Global Custodians, sind alle Befragten bereit, die Umsetzung von einheitlichen Standards zu unterstützen. Nach Aussage der Studienteilnehmer wären diese willens, ihre internen fachlichen und technischen Prozesse anzupassen.

Wir sind zuversichtlich, dass die Asset-Management-Branche es trotz des aktuellen „regulatorischen Tsunamis" schafft, durch weitergehende Vereinbarungen annähernd den Standardisierungs- und Automatisierungsgrad der Logistikbranche zu erreichen, insbesondere mit Unterstützung des BVI.

Mehr Handel durch Standardisierung!



Cloud Computing – der Apfel ist längst angebissen

Neue Herausforderungen in Sachen Sicherheit – spezialisierte Berater gefragt

Stefan Wendt
Partner im Managing Board
microfin Unternehmensberatung GmbH

Die Cloud ist im Kopf von CIOs längst Realität. Sie scheint so viele Probleme zu lösen, mit denen die IT über Jahrzehnte gekämpft hat, dass die IT kaum widerstehen kann. Bedienerfreundlichkeit und Flexibilität sind nur zwei der Stichworte. Hinzu kommen niedrige Kosten und die Befreiung vom Zwang, internes Know-how auch für IT-Aufgaben fern des Kerngeschäfts aufzubauen. So kann die Cloud zunehmend Enabler für die weitere Digitalisierung von Geschäftsmodellen und Prozessen werden. Und trotzdem hängt die Cloud nach wie vor wie der berühmte rotbackige Apfel am Baum, und die Unternehmen ringen mit sich, ob sie ihn pflücken sollen. Speziell Sicherheitsbedenken und Fragen der IT-Compliance treiben sie um – die nach Prism und Co. nicht weniger geworden sind.

Tatsache ist: Der Apfel ist längst angebissen. Der Markt für Cloud Computing legte laut Bitkom allein 2013 um rund 50 % zu. Aber wie beim biblischen Baum der Erkenntnis schwant den IT-Verantwortlichen nach der ersten Genugtuung, dass sie sich mit der Cloud auch ganz neue Herausforderungen in Sachen Sicherheit aufgebürdet haben. Denn: Einheitliche Regeln zum Angebot und zur Nutzung von Cloud-Diensten gibt es (bislang) noch nicht, kompliziert wird es vor allem bei regulierten Branchen wie Banken, Versicherungen und Pharma – insbesondere aus Sicht der IT-Compliance.

Die Bedenken sind berechtigt und nachvollziehbar: Mit zunehmender Fertigungstiefe in der Cloud werden die Möglichkeiten der unmittelbaren Kontrolle und Steuerung der Auslagerung weniger. Was bei „Infrastructure as a Service“ – im Grunde die Bereitstellung reiner Rechenleistung – noch überschaubar erscheint, wird spätestens bei Software as a Service hoch komplex. Ähnliche Unterscheidungen gelten für die verschiedenen Formen der Cloud: Die Private Cloud ist beherrschbar, die Community Cloud oder gar die Public Cloud sind es nicht oder zumindest nur sehr eingeschränkt.

Das bedeutet aber durchaus nicht, dass die Sicherheit und Verfügbarkeit in der Cloud grundsätzlich niedriger sind als bislang üblich. IT-Sicherheitsniveau und Bedrohungsszenarien sind in Cloud-Lösungen oft mit bestehendem On Premise Outsourcing vergleichbar und bieten teilweise sogar bessere Services. Potenzielle Bedrohungen der Daten des auslagernden Unternehmens wegen Datenverlusts oder Missbrauchs bestehen gleichermaßen in der Cloud und außerhalb der Cloud, etwa im eigenen Rechenzentrum. Die Maximal-Standardisierung von Cloud-Lösungen limitiert allerdings die Umsetzbarkeit individueller Abweichungen. Das gilt auch für die Wahrung und Umsetzung der Einzelanforderungen aus der IT-Compliance: In Cloud-Modellen weicht etwa die Governance-Struktur regelmäßig vom marktüblichen Aufbau ab.

Bedenken sind berechtigt und nachvollziehbar

Das kann zum Problem werden, denn klar ist: Compliance-Vorgaben ist es in aller Regel gleichgültig, ob ein Dienst in die Cloud ausgelagert wird oder nicht. Die Anforderungen aus der IT-Compliance sind in weiten Teilen identisch mit dem klassischen IT-Outsourcing. Neben der bereits erwähnten Governance greifen dieselben Kategorien: Datenschutz, IT-Security sowie Business und Service Continuity.

Schon die Leistungsbeschreibungen stellen Unternehmen vor neue Herausforderungen: Cloud-Service-Beschreibungen sind in ihrer Spezifikation meist vergleichbar mit den mit On-Premise-Providern vereinbarten Servicebeschreibungen – sie folgen allerdings in der Regel einer abweichenden Struktur, da die funktionale Servicesicht im Vordergrund steht. Daher ist eine Überprüfung unerlässlich, ob Servicemerkmale und Aktivitäten durchgängig beschrieben, erforderliche Mitwirkungen des auslagernden Unternehmens gekennzeichnet sind

und für Service Level Agreements präzise Definitionen, Schwellenwerte und Messmethoden vereinbart wurden. Im Gegensatz zum On Premise Outsourcing werden im Cloud Sourcing typischerweise die Vertragsstandards des Anbieters verwendet. Eine Herausforderung ergibt sich häufig auch aus dem Umstand, dass vom Cloud-Service-Provider – abweichend zum On Premise Outsourcing – keine festen Ansprechpartner benannt werden.

Alle wesentlichen Aspekte müssen bereits im Vorfeld bekannt und bewertet sein, damit eine Cloud-Einführung langfristig erfolgreich abläuft. Entscheidend dafür ist eine solide Vorbereitung auch aus Sicht der IT-Compliance. Fünf Punkte haben sich dabei in der Praxis als wesentlich herausgestellt:

1. **Mündliche Ausführungen** des Cloud-Service-Providers – insbesondere zu Aspekten von Datenschutz und IT-Security – hartnäckig hinterfragen, schriftlich belegen und im Zweifel vertraglich zusichern lassen.
2. **Zwingende Vorgaben** (wie Datenschutz oder interne IT-Security-Policy) und deren Umsetzung durch den Cloud-Service-Provider in der Cloud-Lösung fest vereinbaren.
3. Die **Servicebeschreibung** der Cloud-Lösung auf Mindestinhalte (funktional-technische Beschreibung, SLAs, Mitwirkungsleistungen etc.) prüfen und eine verbindliche Informationspflicht des Cloud-Service-Providers bei Änderungen und/oder Ergänzungen vertraglich zusichern lassen.
4. **Exit-Szenarien** schon vor dem Start dokumentieren und kontinuierlich aktualisieren, um im Falle der Remigration auf „on premise“ sofort handlungsfähig und flexibel zu sein.
5. Den **Reifegrad der eigenen Organisation für Cloud-Lösungen** hinterfragen und dauerhaft ausbauen, um in allen Bereichen der Organisation (IT, Recht, Revision) über dasselbe Verständnis zu verfügen.

Keine triviale Aufgabe

Eine Migration in die Cloud compliancegerecht umzusetzen, ist also keine triviale Aufgabe. Sie kann sich, operativ gesehen, lohnen – wenn ihre Risiken in jeder Hinsicht kontrollierbar bleiben. Kein Zufall also, dass sich Unternehmen noch skeptisch zeigen und sich vor dem Schritt in die Cloud die Erfahrung von spezialisierten Beratern zunutze machen. Denn so verlockend der Apfel ist: Man sollte vor dem ersten Bissen schon wissen, dass er wirklich nicht verboten ist.

Vertrauen genügt nicht für eine erfolgreiche Outsourcing-Partnerschaft

Klare Regeln sind das A und O – Gemeinsame Sicht ist eine zwingende Voraussetzung

Dr. Gerald Spiegel
Senior Manager bei
Steria Mummert Consulting
im Bereich Information
Security Solutions

Unternehmen beauftragen heute eine Vielzahl von Dienstleistern damit, unterschiedliche IT-Leistungen für sie zu übernehmen. Die Bandbreite reicht von der Notfallvorsorge und dem Betrieb von IT-Infrastruktur und Anwendungen über die Anwendungsentwicklung bis hin zur Auslagerung ganzer Geschäftsprozesse. Eine der größten Herausforderungen für die Outsourcing-Partner ist es dabei, Ausfall- und Informationssicherheit zu gewährleisten und die entsprechende Kontrolle und Überwachung zu organisieren.

Unternehmen verfolgen mit Outsourcing neben Kosteneinsparung häufig auch die Strategie einer Risikoübertragung – ähnlich wie mit dem Abschluss einer Versicherung. Diese Strategie ist jedoch nur dann erfolgreich, wenn auch die durch das Outsourcing selbst entstehenden Risiken erkannt und gehandhabt werden. Im Einzelnen sind dies:

- **Brain Drain:** Know-how wandert aus dem Unternehmen zum Dienstleister ab. Dieses Wissen fehlt dem Auftraggeber dann, wenn sich mit dem Outsourcing-Partner Probleme ergeben, oder auch schon wenn es darum geht, die Leistungen des externen Dienstleisters hinsichtlich Qualität und Werthaltigkeit zu beurteilen.
- **Abhängigkeit vom Dienstleister:** Die Insolvenz eines Netzbetreibers kann beispielsweise dazu führen, dass das komplette Firmennetzwerk nicht mehr verfügbar ist.
- **Fehlendes oder mangelhaftes Outsourcing Management:** Dies führt zu lückenhaften Verträgen – insbesondere bezüglich Service Level Agreements – und zu nicht ausreichender Überwachung der Dienstleistung.
- **Fehlende Sicherheitsarchitektur beim Dienstleister:** Das kann zu Vertraulichkeits- oder Integritätsverlust bei den Unternehmensdaten oder sogar zum Verstoß gegen einschlägige Gesetze führen.

Riskante Irrtümer

In der Praxis erschweren Vorurteile das Management der Risiken von Outsourcing-Partnerschaften häufig. Ein weitverbreiteter Irrtum besteht zum Beispiel darin, dass der Outsourcing-Partner die volle Verantwortung für die Informationssicherheit übernimmt. Diese Verantwortung lässt sich jedoch grundsätzlich nicht auslagern, sondern verbleibt bei der Leitung des Auftraggebers. Externe Dienstleister übernehmen stets nur vertraglich festgelegte Aufgaben und Rollen. Der Umfang und die Gestaltung dieser Leistungen sowie deren Kontrolle liegen aber beim auslagernden Unternehmen.

Darüber hinaus betrachten Servicenehmer Informations- und Ausfallsicherheit häufig als rein technische Angelegenheit, die man scheinbar noch nach Vertragsabschluss mit dem Partner regeln kann. Diese Fehleinschätzung resultiert oft aus dem mangelnden Verständnis für die Notwendigkeit einer eigenen Sicherheitsorganisation und eines eigenen Regelwerks. Viele auslagernde Firmen glauben immer noch: Wer für welche Aufgaben zuständig ist, lasse sich mit etwas Vertrauen in den Partner schon regeln. Dies trifft insbesondere dann zu, wenn die Mitarbeiter des Dienstleisters ehemalige Mitarbeiter des Auftraggebers sind und per Betriebsübergang zum Dienstleister gewechselt sind.

Vertrauen ist zwar notwendig, genügt aber nicht für eine erfolgreiche Outsourcing-Partnerschaft. Klare Absprachen, die die Kunden-Lieferanten-Beziehung detailliert beschreiben, schriftlich fixiert in einem Vertragswerk, sind unabdingbar. In solch einem Regelwerk sollte beispielsweise eine genaue Rollen- und Berechtigungsdefinition enthalten sein.

Außerdem sollte darin enthalten sein, dass der Auftraggeber die verabredeten Sicherheitsmaßnahmen beim Dienstleister regelmäßig über-

prüfen darf. Denn mangelnde Kontrolle durch den Servicenehmer birgt immer das Risiko, dass der Servicegeber festgelegte Abwehrmaßnahmen gegen Ausfälle und Datenabflüsse schleichend und unbemerkt vernachlässigt.

Das Regelwerk sollte unter anderem die folgenden Einzelpunkte in der Vertragsgestaltung berücksichtigen:

- Es muss exakt festhalten, wer Eigentümer von Informationen, Arbeitsergebnissen und Systemkomponenten ist. Bei einer externen Anwendungsentwicklung ist zu vereinbaren, ob der Dienstleister weitere Nutzungsrechte an der von ihm erstellten Software hat.
- Der Dienstleister sollte Maßnahmen nachweisen, mit denen er seine Mitarbeiter sensibilisiert und kontrolliert. Er sollte Auskunft darüber geben, wie seine Mitarbeiter für die vereinbarte Datensicherheit sorgen und wie vertrauensvoll sie mit Informationen umgehen. Eine Vertraulichkeitserklärung ist das absolute Minimum, besser aber sind regelmäßige Kontrollen durch den Auftraggeber.
- Eine Notfall- und Mangeldefinition empfiehlt sich ebenfalls. Sie enthält Bedingungen, anhand derer eine Störung oder ein Notfall qualifiziert werden kann. Hilfreich ist ein Schema mit Fehlerklassen, aus dem auch Reaktionszeiten zur Mängelbeseitigung hervorgehen.
- Eine genau definierte Vorgehensweise bei Vertragsablauf und Kündigung stellt sicher, dass die Vertraulichkeit von Informationen auch nach Auflösung des Vertragsverhältnisses gewährleistet ist.
- Vereinbarungen sollten sich schnell anpassen lassen, um künftigen Anforderungen gerecht zu werden.

Beim IT-Outsourcing drohen viele Risiken, deshalb lohnt es sich, genau hinzusehen.

Je klarer die vertraglichen Regeln sind, desto besser lassen sie sich nachprüfen und messen. Wenn beispielsweise nur ein bestimmter Mitarbeiter auf das Firmennetzwerk des Kunden zugreifen darf, sollte das auch so festgehalten werden. Denn dann lässt sich später anhand von Protokolldateien feststellen, welcher Mitarbeiter tatsächlich auf die IT-Systeme des Auftraggebers zugegriffen und sich in seinen Netzwerken bewegt hat. Wenn möglich, sollten Kontrollen softwareunterstützt und kontinuierlich durchgeführt werden. Spezielle Auditierungsprogramme helfen dabei, das geforderte Sicherheitsniveau regelmäßig zu prüfen.

Im Idealfall orientieren sich die mit dem Outsourcing-Partner vereinbarten Kontrollsysteme an anerkannten Standards wie ISO 27001, den BSI Grundschutzkatalogen oder den Control Objectives for Information and Related Technology (COBIT). Auch ITIL kann unterstützen, zum Beispiel bei der Vermeidung von Risiken, indem Themen wie Security Management, Configuration Management und Service Level Agreements (SLAs) beschrieben werden. Auch im internationalen Standard ISO 27002 werden Sicherheitsaspekte bei Outsourcing-Verträgen und Inhalte von Service Level Agreements aufgegriffen – basierend auf allgemeinen Regeln und Bedingungen für Verträge mit Fremdfirmen.

Ein gemeinsames Verständnis der Ziele, Aufgaben, Rollen und Risiken beim Outsourcing ist eine zwingende Voraussetzung einer für Auftraggeber und Outsourcing-Dienstleister gewinnbringenden und langfristigen Zusammenarbeit. Diese gemeinsame Sicht herzustellen ist keine triviale Aufgabe.

Um den Prozess zu erleichtern, kann es sinnvoll sein, dass die Partner eine unabhängige Partei als Vermittler bestimmen. Diese neutrale Instanz „übersetzt“ die geschäftlichen Anforderungen des Servicenehmers in geeignete und angemessene technische und organisatorische Maßnahmen beim Servicegeber.

concedro
BUSINESS FORWARD

Lassen Sie uns gemeinsam
Ihr »Business Forward« bringen.

WIR BRINGEN IHR BUSINESS FORWARD

concedro GmbH ist eine auf die Finanzdienstleistungsbranche spezialisierte Unternehmensberatung. Unsere Expertise umfasst Kapitalmarkt- und Wertpapierprozesse sowie In- und Outsourcing Vorgänge – aus fachlicher und technischer Sicht. Profitieren auch Sie von unserem langjährigen Branchen-Know-how und unserer Management-Erfahrung.

INDIVIDUELL | ERFAHREN | GANZHEITLICH | INTEGRATIV

concedro GmbH | Ulmenstr. 22 / 60325 Frankfurt am Main | EMAIL direct@concedro.com WEB concedro.com