

Wieland Kirch / Gerrit-Leonhard Stein



Die Anforderungen aus Gesetzen und Normen (Compliance) an Gesellschaften

und ihre Organe nehmen seit einigen Jahren kontinuierlich zu. Unternehmen, die ihre Prozesse und Services im Outsourcing betreiben, erhalten häufig keine adäquate Hilfestellung von ihrem Dienstleister, diese Anforderungen zu erfüllen. Was können die Dienstleister tun, um ihre Kunden durch zielgerichtetes Risikomanagement sinnvoll zu unterstützen? Kann das kundenbezogene Risikomanagement als Wettbewerbsvorteil genutzt werden?

Compliance-Anforderungen und ihre Folgen

Die Auslagerung von rechnungslegungsrelevanten Dienstleistungen (Outsourcing) nimmt durch den technologischen Fortschritt laufend zu. Durch die wachsenden technischen Möglichkeiten verändern sich auch die Qualitäten der Dienstleistungen. Wurden anfangs nur leicht standardisierbare Unterstützungsprozesse (zum Beispiel Rechenzentrumsleistungen) ausgelagert, geht heute der Trend zur Auslagerung ganzer betrieblicher Funktionen (Shared Service Center) und Hauptgeschäftsprozesse (Business Process Outsourcing).

Mit zunehmender Komplexität der Dienstleistungen gewinnt auch die Beachtung der Compliance in diesem Zusammenhang für Auslagernde und Dienstleister an Bedeutung und erfordert entsprechende Konkretisierungen in den Dienstleistungsverträgen und Service Level Agreements (SLA).

Compliance-Pflichten können nicht an den Dienstleister delegiert werden, auch wenn

Das Risiko bei Auslagerungen richtig überwachen

Prüfungsstandard

Im Zusammenhang mit Outsourcing-Maßnahmen sehen sich die auslagernden Unternehmen einer großen Anzahl von Compliance-Vorschriften gegenüber – genau wie die Verantwortung für die abgegebenen Prozesse kann auch die Prüfung der Einhaltung von Gesetzen und Normen nicht vom aufnehmenden Dienstleister übernommen werden. Insbesondere das Risikomanagement beim Serviceprovider, so konstatieren die Autoren, stellt sich für den Auslagernden und dessen Abschlussprüfer oft als eine Blackbox dar. Um dem entgegenzuwirken skizzieren sie die Elemente des im September 2007 eingeführten Prüfungsstandards IDW PS 951, durch den die Erfüllung von Compliance-Anforderungen dokumentiert und sichergestellt werden soll. (Red.)

diese in den Verträgen erwähnt und konkretisiert wurden. Verantwortlich bleiben in jedem Fall die geschäftsführenden Organe der auslagernden Gesellschaft. Zu den wichtigsten allgemeingültigen Compliance-Pflichten gehören:

- Einrichtung ordnungsmäßiger und sicherer Rechnungslegungssysteme (Stichwort Grundsätze ordnungsmäßiger Buchführung, GoB).

Die Autoren

Gerrit-Leonhard Stein, Senior Manager, Helbling Management Consulting GmbH, Eschborn, und Wieland Kirch, Partner, Schomerus & Partner, Hamburg

- Einrichtung eines angemessenen Risikomanagements (Stichwort Interne Kontrollsysteme, IKS).

Hinzu kommen oft weitere Spezialnormen in Abhängigkeit von Rechtsform und Geschäft wie zum Beispiel:

- Gesteigerte Anforderungen an die Zulässigkeit von Auslagerungen von Dienstleistungen (MaRisk).

- Gesteigerte Dokumentations- und Nachweispflichten betreffend das Risikomanagement im Umfeld von Tochtergesellschaften oder Dienstleistern von US-Gesellschaften (Sarbanes-Oxley Act – SOX).

- Kreditvergaberichtlinien und deren indirekte Anforderungen an die Organisationsqualität und das eingesetzte Risikomanagement (Basel II).

- Regelwert für die Datensicherheit bei der Abwicklung von Kreditkartentransaktionen (Payment Card Industry Data Security Standard – PCI).

Risikomanagement oft Blackbox

Das Risikomanagement beim Provider für die ausgelagerte Dienstleistung stellt sich für den Auslagernden und dessen Abschlussprüfer oft als eine Blackbox dar. Durch die sich laufend verschärfenden Compliance-Anforderungen müssen sich jedoch Auslagernder und dessen Abschlussprüfer intensiv mit der Qualität dieses Risikomanagements auseinandersetzen. Für den Dienstleister (Provider) entstehen aus diesem Kundenanspruch Anforderungen an sein Risikomanagement und umfangreiche Nachweispflichten.

Der gelebte Umgang mit den Compliance-Pflichten ist in der Praxis in vielen Unter-

nehmen unabhängig von Größe, Rechtsform und Branche häufig sehr ähnlich und oft unbefriedigend. Berater und Wirtschaftsprüfer stellen im Allgemeinen immer wieder die gleichen Aspekte fest:

Sicht des Abschlussprüfers des Auslagernden

In der Praxis wird der Abschlussprüfer oft mit einer unzureichenden Dokumentation des Risikomanagements konfrontiert. Er muss sich unabhängig von der Existenz und Qualität dieser Dokumentation ein Bild über die Risiken und korrespondierenden Kontrollmaßnahmen seines Mandanten machen. Im Rahmen dieser Aufgabe ist er gezwungen, die fehlende Dokumentation partiell nachzuholen oder das Fehlen entsprechend zu beanstanden. Folgende Dokumentationen fehlen häufig oder sind zumindest oft unvollständig und inaktuell: Definition der Risiken und der korrespondierend eingerichteten Kontrollmaßnahmen, Prozessbeschreibungen, Verfahrens- und Anwenderdokumentation von Rechnungslegungssystemen.

Intensive Bemühungen von deutschen Gesellschaften und deren Abschlussprüfern zur Verbesserung dieser Dokumentationschwächen sind in letzter Zeit insbesondere bei Tochtergesellschaften oder Dienstleistern amerikanischer Gesellschaften aus dem SOX-Umfeld zu beobachten.

Besondere Informationsdefizite existieren erfahrungsgemäß im Bereich der ausgelagerten rechnungslegungsrelevanten Bereiche. Auch hier fehlt häufig eine geeignete Dokumentation des Risikomanagements

und der Prozesse. Hinzu kommt aber, dass es vertraglich oder auch praktisch häufig nicht oder nur eingeschränkt möglich ist, sich die Informationen direkt beim Dienstleister zu verschaffen. Diese Informationsdefizite führten bisher nur selten zu gravierenden Beanstandungen der Abschlussprüfer. Hiermit ist aber in Zukunft aufgrund strengerer Normen zu rechnen. Qualitätsnachweise analog des amerikanischen Prüfungsstandards SAS 70 gibt es in Deutschland bisher nur im Ausnahmefall soweit eben durch SOX erzwungen.

Sicht des Auslagernden

Die Anforderungen des Auslagernden hinsichtlich Effektivität und Effizienz der Prozesse, Gewährleistung einer ordnungsmäßigen Rechnungslegung sowie Einhaltung von Compliance werden in Dienstleistungsverträgen oft nicht ausreichend definiert. Die ausgelagerten Prozesse und das zugehörige Risikomanagement sind für den Auslagernden deshalb oft nicht transparent. Es fehlt auch hier oft an einer geeigneten Dokumentation.

Das auslagernde Unternehmen sollte aufgrund bestehender Compliance-Pflichten kontinuierlich und nicht nur im Rahmen des Vertragsabschlusses dafür Sorge tragen, dass ein geeignetes Risikomanagement eingerichtet ist. Soweit die Geschäftsleitung dieser Aufgabe nicht persönlich nachkommen möchte, bietet es sich zumindest für komplexere Sachverhalte an, damit die interne oder eine externe Revision zu beauftragen. Diese Überwachung sollte unabhängig von den Jahresabschlussprüfungen regelmäßig aus-

geübt werden und bei Bedarf zu Anpassungen des Risikomanagements führen.

Im Bereich der Unternehmensüberwachung durch die Geschäftsführung oder „Interne Revision“ besteht bei vielen Unternehmen insbesondere bei Mittelständlern akuter Handlungsbedarf.

Sicht des Dienstleisters

Ohne konkrete Vorgaben auf Basis der individuellen Risikoeinschätzung des Auslagernden können Dienstleister kein optimales Risikomanagement der Dienstleistung etablieren.

Der Dienstleister hat nur dann an einer Optimierung des dienstleistungsbezogenen Risikomanagements Interesse, wenn dieser Zusatzaufwand geschätzt und honoriert wird. Dies ist jedoch nur dann der Fall, wenn der Zusatznutzen zur Optimierung des dienstleistungsbezogenen Risikomanagements (Beratung, Information und Qualitätsnachweis) entsprechend vermarktet und dem Kunden als notwendiger Service dargestellt wird.

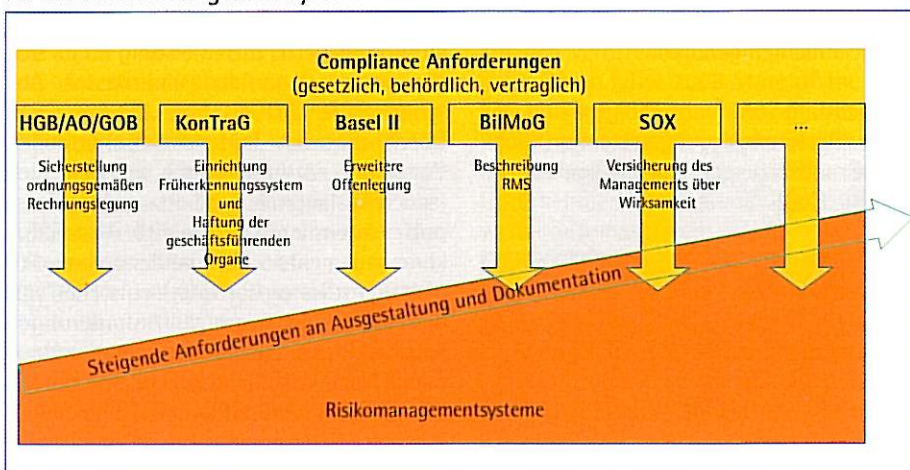
Auch wenn der Dienstleister nicht originär die Compliance-Anforderungen seiner Kunden erfüllen muss, steigen zumindest indirekt die vertraglichen Anforderungen und damit kontinuierlich die Haftungsrisiken. Somit besteht für die Dienstleister schon aus Wettbewerbsaspekten ein entsprechender Handlungsbedarf.

Auslagerung der Prüfung als Lösungsansatz

Eine externe Überprüfung des Risikomanagements für die ausgelagerte Dienstleistung bringt dem Provider viele Vorteile:

- Die externe Prüfung des Risikomanagements des Providers steigert die Effizienz und Effektivität: Sofern der Dienstleister mehrere vergleichbare Kunden hat, ist es effizienter, wenn das dienstleistungsbezogene Risikomanagementsystem nur einmal stellvertretend für alle Dienstleistungsempfänger untersucht wird. Durch die Auslagerung wird es wirtschaftlich möglich, tendenziell intensiver und damit auch effektiver zu prüfen.
- Auslagerung der Prüfung sichert Vertraulichkeit: Durch die Auslagerung der Prüfung kann leichter sichergestellt wer-

Abbildung 1: Steigende Compliance-Anforderungen an das Risikomanagementsystem



den, dass vertrauliche Informationen, die nicht das dienstleistungsbezogene Risikomanagement betreffen, nicht in falsche Hände gelangen.

- Marketingnutzen durch externen Qualitätsnachweis: Auslagerung der Prüfung kann als Qualitätsnachweis des dienstleistungsbezogenen Risikomanagements zu Marketingzwecken verwendet werden.

Das Institut der Wirtschaftsprüfer hat auf Basis des amerikanischen Prüfungsstandards SAS 70 unter Berücksichtigung nationaler Besonderheiten einen Prüfungsstandard PS 951 im September 2007 herausgebracht. Die Verwendung bietet sich sowohl im SOX-Umfeld wie auch für viele Dienstleistungsanbieter in Deutschland an.

Durch eine Bescheinigung Typ B nach PS 951 bestätigt der Wirtschaftsprüfer hinsichtlich des dienstleistungsbezogenen Risikomanagements das Folgende:

- Die Risiken und Kontrollen sind richtig und klar in einer Berichtsanlage beschrieben.
- Die Kontrollen waren zu einem definierten Zeitpunkt eingerichtet.
- Die Kontrollen sind prinzipiell geeignet, die Risiken abzudecken.
- Die Kontrollen waren während des Untersuchungszeitraums wirksam.
- Die Kontrollziele haben mit hinreichender Sicherheit die Risiken abgedeckt.

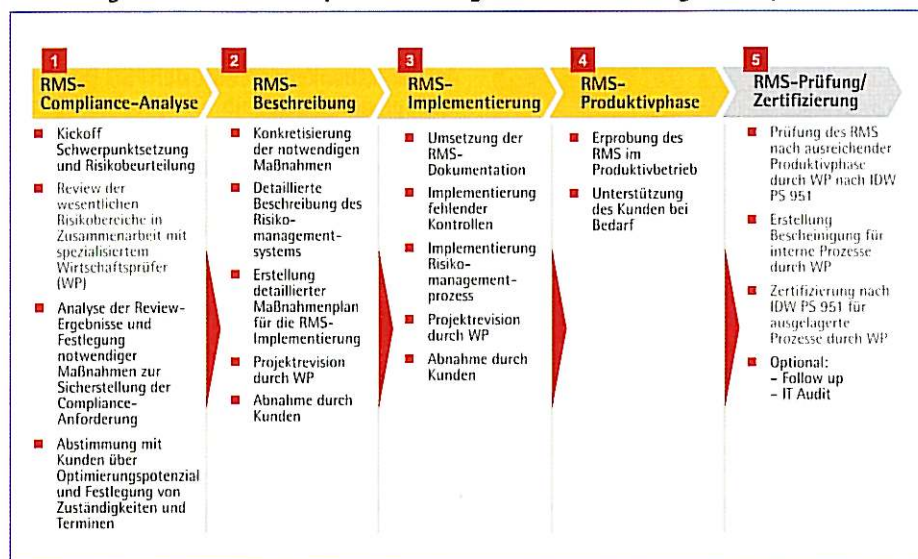
Der Abschlussprüfer des Auslagernden darf einen Bericht nach IDW PS 951 Typ B verwenden, um eine Einschätzung des Fehlerrisikos vorzunehmen und kann im Idealfall auf weitere Prüfungshandlungen in dem betreffenden Bereich vollständig verzichten.

Realisierung und Prüfung eines Risikomanagementsystems

Für die Umsetzung eines entsprechend dokumentierten Risikomanagementsystems (RMS) zur Sicherstellung der Compliance-Anforderung und einer anschließend erfolgreichen Bescheinigung, sind vier Phasen notwendig:

Phase 1: Analyse der Compliance-Risiken und Festlegung der notwendigen Maßnahmen: Zuerst müssen die wesent-

Abbildung 2: Prozesse zur Implementierung eines Risikomanagementsystems



lichen Compliance-Risikobereiche für die Outsourcing-Leistung identifiziert werden. Anschließend folgen dann eine Analyse der Risikobereiche und die Festlegung eines Maßnahmenplans. Der für die Zertifizierung zuständige Wirtschaftsprüfer sollte projektbegleitend in den Realisierungsprozess miteingebunden werden, damit die notwendige Qualität im gesamten Prozess sichergestellt und der dafür erforderliche Aufwand optimiert werden kann.

Phase 2: Beschreibung eines dienstleistungsbezogenen Risikomanagementsystems: Auf Basis des in Phase 1 erstellten Maßnahmenplans erfolgt in Phase 2 die Konkretisierung der notwendigen Maßnahmen zur Sicherstellung der Compliance-Anforderung. Zusätzlich ist es notwendig, eine umfassende Beschreibung des RMS zu erstellen und hierfür einen entsprechenden detaillierten Maßnahmenplan für die RMS-Implementierung anzufertigen.

Phase 3: Implementierung des dienstleistungsbezogenen RMS: In der dritten Phase erfolgt die Realisierung des RMS. Insbesondere werden die notwendigen und oft nicht vorhandenen Dokumentationen erstellt, fehlende Kontrollen ergänzt und ein umfassender Risikomanagement-Prozess implementiert.

Phase 4: Prüfung und Bescheinigung des dienstleistungsbezogenen RMS durch unabhängigen Wirtschaftsprüfer: Nach erstmaliger Einrichtung kann der zuständige Wirtschaftsprüfer eine Bescheinigung über die Qualität des neuen Sollsystems

(Typ A-Bescheinigung) als Abschluss der Implementierungsphase erteilen.

Nach einer Produktivphase von etwa zwölf Monaten, in der die Wirksamkeit des implementierten RMS unter Beweis gestellt werden muss, kann der zuständige Wirtschaftsprüfer zusätzlich auch die Funktionsfähigkeit des Risikomanagementsystems für die ausgelagerten Dienstleistungen für diese Periode bestätigen. Diese höherwertige Bescheinigung (Typ B) dient dem Provider, die Qualität seines RMS seinen Kunden und deren Abschlussprüfern zu bestätigen.

Nutzen von Kunden und Dienstleistern

In einem Umfeld, mit immer stärkeren Compliance-Anforderungen an die Unternehmen, müssen Outsourcing-Kunden und -Provider aktives Risikomanagement betreiben. Hierfür erforderlich sind geeignete Dokumentationen von Prozessen und Systemen, die Verwendung von anerkannten Risikomanagement-Prozessmodellen, eine Präzisierung der Verträge und SLAs.

Provider sollten die Chancen des Prüfungsstandards IDW PS 951 durch die Auslagerung der RMS-Prüfung erkennen und aktiv für sich und ihre Kunden nutzen. Die bisher sanktionslose Nichtbeachtung von Compliance-Anforderungen könnte sich künftig zu einem wesentlichen Risiko für die Kunden im Outsourcing-Umfeld entwickeln. Aufgrund der vertraglichen Haftung können die Probleme der Kunden schnell zum Problem der Provider und für diese zu Wettbewerbsnachteilen führen.