

# Outsourcing braucht Kontrolle

Anwender sollten auf ein zertifiziertes Kontrollsystem ihres Providers achten. Nur so können sie die rechtlichen Anforderungen erfüllen, für die sie selbst haften.

VON GERRIT-LEONHARD STEIN\*

Die Compliance-Anforderungen steigen ständig. Neben gesetzlichen und behördlichen Auflagen wie HGB-Richtlinien oder KontraG müssen Unternehmen immer mehr branchenspezifischen Anforderungen – etwa Basel II – sowie den jeweiligen Standards der Industrie gerecht werden. Für Versäumnisse in dieser Hinsicht haften in der Regel die Geschäftsführer. Das gilt auch dann, wenn das Unternehmen bestimmte Geschäftsprozesse und Funktionen an einen externen Provider ausgelagert hat. Die Verantwortung dafür, Gesetze einzuhalten, kann er nicht an den Outsourcing-Anbieter delegieren. Anwender müssen Compliance-Anforderungen im Rahmen ihrer Sourcing-Entscheidung im Auge behalten.

## Hier lesen Sie ...

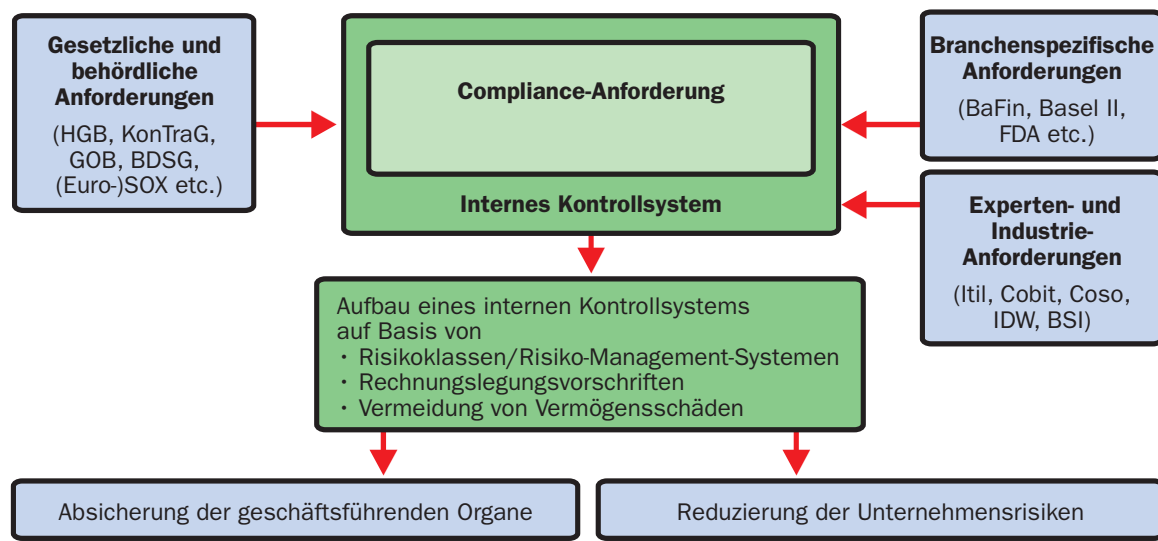
- ◆ welche Compliance-Anforderungen auch im Outsourcing gelten;
- ◆ warum IT-Dienstleister den Kunden ungern Prüfungsrechte einräumen;
- ◆ wie sich interne Kontrollsysteme als Alternative implementieren lassen.

Allerdings lassen sich die Leistungen, die der Provider erbringt, meist nur indirekt steuern und kontrollieren. Der Anwender sollte daher möglichst schon vor Unterzeichnung des Outsourcing-Vertrags sicherstellen, dass der Provider mit der gleichen Sorgfalt und den notwendigen Kontrollmechanismen arbeitet, die für den Auftraggeber verbindlich sind. Das heißt, die Schnittstellen zwischen den internen Kontrollsystemen des Outsourcing-Kunden und denen seines Providers sind so zu definieren, dass der Anwender die Einhaltung der Compliance-Kriterien auch für die in externen IT-Systemen umgesetzten Prozesse nachweisen kann.

## Verantwortung klar verteilen

Das setzt voraus, dass Outsourcing-Auftraggeber und Provider klare vertragliche Regelungen treffen. Je nachdem, welche Anforderungen der Kunde erfüllen muss, lassen sich diese unter Umständen in Form von SLAs (Service-Level-Agreements) und

## Rechtssicherheit durch ein Kontrollsystem



Das interne und von unabhängigen Prüfern zertifizierte Kontrollsystem gewährleistet, dass Anwenderunternehmen auch im Outsourcing-Betrieb die an sie gestellten Compliance-Anforderungen erfüllen.

KPIs (Key-Performance-Indicators) gewährleisten. Dabei sollte der Kunde mit seinem Provider eine klare Rollenverteilung mit eindeutigen Verantwortlichkeiten vereinbaren und ihm die gesetzlichen und regulatorischen Anforderungen präzise vorgeben. Ziel sollte sein, dass der Dienstleister die dafür erforderlichen Kontrollpunkte in seinen Prozessen berücksichtigt und dem Kunden einen entsprechenden Qualitätsnachweis erbringt. Das können beispielsweise Verfügbarkeitsstatistiken oder Fehler-Reports über verbuchte Daten sein.

Große Anwenderunternehmen, die besonders hohen gesetzlichen und/oder regulatorischen Anforderungen gerecht

werden müssen, haben aber noch weitere Möglichkeiten, um sicherzustellen, dass der Provider die entsprechenden Kontrollmechanismen etabliert hat. So kann der Dienstleister dem Kunden beziehungsweise dessen Wirtschaftsprüfer ein Prüfungsrecht einräumen.

## Prüfungsrecht für Anwender

Die meisten Anwenderunternehmen versäumen es jedoch, sich dieses Recht bei Unterzeichnung des Outsourcing-Vertrags schriftlich zusichern zu lassen. Die Serviceanbieter werden sich nicht grämen, ist mit dieser Variante doch ein hohes Risiko für sie verbunden: Gewähren sie dem Auftraggeber ein Prüfungsrecht, legen sie damit zwangsläufig ihre

## In vier Phasen zum Kontrollsystem

■ **Phase 1:** Definition der Risikobereiche. Zunächst muss der Anwender die Compliance-relevanten Risikobereiche für die jeweilige Outsourcing-Leistung identifizieren und anschließend mit einem spezialisierten Wirtschaftsprüfer abstimmen. Darauf folgen die Analyse der Risikobereiche und die Festlegung eines entsprechenden Masterplans zur Sicherstellung der Compliance-Einhaltung. Auch hier empfiehlt sich eine anschließende Abstimmung des Masterplans mit dem Wirtschaftsprüfer.

■ **Phase 2:** Beschreibung eines dienstleistungsbezogenen internen Kontrollsystems. Auf Basis des Masterplans werden die Maßnahmen entwickelt, die die Erfüllung der Compliance-Anforderungen sicherstellen. Wichtig dabei ist es, das interne Kontrollsystem zunächst einmal umfassend zu beschreiben.

■ **Phase 3:** Implementierung des internen Kontrollsystems. In der dritten Phase erfolgt die Realisierung des internen Kontrollsystems auf Basis der Maßnahmenpläne.

■ **Phase 4:** Prüfung und Bescheinigung des internen Kontrollsystems durch den Wirtschaftsprüfer - Wenn die Wirksamkeit des implementierten internen Kontrollsystems unter Beweis gestellt worden ist, erfolgt die Zertifizierung durch den Wirtschaftsprüfer.

Systeme und internen Prozesse sowie letztlich ihre interne Kalkulationsgrundlage offen. Zudem läuft der Provider Gefahr, dass die Wirtschaftsprüfer auch Einblick in die Geschäftsbeziehung zu anderen Kunden erhalten. Damit kann der Serviceanbieter die Basisforderung seiner Auftragnehmer nach Vertraulichkeit nicht mehr erfüllen. Vor diesem Hintergrund wird der Servicelieferant in der Praxis das Prüfungsrecht verweigern und stattdessen Alternativen anbieten.

Besser und ebenfalls sicher ist daher die Variante, dass der Provider dem Anwender ein von einem unabhängigen Wirtschaftsprüfer ausgestelltes Zertifikat vorlegt, das ihm einwandfrei funktionierende Kontrollsysteme bescheinigt. Voraussetzung dafür ist, dass der Provider ein internes Kontrollsystem für die jeweilige Dienstleistung etabliert – etwa im Rahmen des Availability-Managements im Itil-Framework oder der Control-Objectives im Cobit-Modell.

## Unabhängiges Zertifikat

Um das interne Kontrollsystem nachzuweisen, empfiehlt sich der neue Prüfungsstandard IDW PS 951, der nach dem Vorbild des US-amerikanischen SAS 70 für die Gegebenheiten des deutschen Markts konzipiert wurde. Mit Hilfe dieses Standards kann der Wirtschaftsprüfer das rechnungslegungsrelevante interne Kontrollsystem einer ausgelagerten Dienstleistung prüfen und bescheinigen. Ein weiterer Vorteil des IDW-Standards besteht dar-

in, dass er auch den Anforderungen, die der Sarbanes-Oxley Act (SOX) etwa an Tochterfirmen von US-Konzernen stellt, gerecht wird.

## Hilfe vom Service-Provider

Wegen der zunehmenden Anforderungen an die Unternehmen müssen Outsourcing-Anwender und ihre Provider dafür sorgen, ihr jeweiliges Geschäftsrisiko aktiv zu reduzieren. Die Verantwortung für die Umsetzung der Compliance-Anforderungen trägt zwar grundsätzlich der Anwender. Der Provider kann ihm aber durch die Implementierung, Dokumentation und Zertifizierung von internen Kontrollsystemen für die ausgelagerten Prozesse und Services entsprechende Sicherheitsnachweise garantieren. (sp) ◆

## So wirkt das Kontrollsystem

### Dem Anwender bietet das Kontrollsystem

- die Gewähr, dass ausgelagerte Prozesse und Funktionen Compliance-Anforderungen erfüllen;
- Schutz vor zusätzlichem Prüfungsaufwand und damit verbundenen Kosten;
- Transparenz der ausgelagerten Prozesse;
- eindeutige Qualitätsnachweise zur Leistungs- und Funktionsfähigkeit des Providers.

### Dem Outsourcing-Anbieter bietet das Kontrollsystem

- eine Alternative zu den Prüfungsrechten des Auftraggebers. Provider vermeiden zudem Mehrfachprüfungen durch Kunden und deren Abschlussprüfer;
- die notwendige Vertraulichkeit gegenüber den Kunden;
- Schutz davor, die interne Kalkulationsgrundlage offenlegen zu müssen;
- eine verbesserte Dienstleistungsqualität durch aktive Prüfung;
- Vermarktungsmöglichkeiten der Compliance-Transparenz und der von unabhängiger Seite geprüften Sicherheit.



\*GERRIT-LEONHARD STEIN ist Senior Manager bei der Helbling

Management Consulting GmbH in Eschborn.