

Compliance im IT-Outsourcing

Betrachtungen zur Vertragsgestaltung und zu aktuellen Entwicklungen

Dr. Michael Heym / Martin Seeburg*

Die Verantwortung bleibt im Haus, die Durchführung geht raus. So einfach lassen sich die vielfältigen Fragestellungen zur Compliance im IT-Outsourcing begründen. Eine große Zahl von Rechtsnormen, Standards sowie Good oder Best Practices können zu beachten sein, und die Wahrscheinlichkeit ist groß, auch während der Laufzeit eines IT-Outsourcing-Vertrags mehrere Änderungen der Compliance-Anforderungen zu erleben. Dies zeigen auch die aktuellen Entwicklungen. Der Schlüssel zur fortwährenden Compliance liegt in der richtigen Vertragsgestaltung.

1. Problemstellung

Outsourcing ist heutzutage ein etablierter Teil der Unternehmensstrategie und kaum ein Unternehmen kommt mehr umhin, sich mit Fragestellungen zum Outsourcing auseinanderzusetzen. Viele Unternehmen im deutschsprachigen Raum haben im IT-Infrastruktur-Outsourcing bereits die zweite oder dritte Generation von Verträgen geschlossen. Das Outsourcing von IT-Anwendungsmanagement ist getrieben durch die möglichen signifikanten Kostenvorteile des Near- oder Offshorings und durch den enger werdenden Personalmarkt für Spezialisten deutlich im Kommen. Es wird in den nächsten Jahren ein großes Thema sein.

Während die Sicherstellung der Compliance im eigenen Unternehmen schon eine Herausforderung ist, ergibt sich durch das Outsourcing der IT ein zusätzlicher Grad an Komplexität. Im Wesentlichen ist dies dadurch begründet, dass Verantwortung beim Auftraggeber verbleibt, diese aber durch den Auftragnehmer auf der Basis von Verträgen und einer gemeinsamen Vertrags-Governance erfüllt werden soll.¹ Beispiele hierfür sind das interne Kontrollsystem (IKS) mit Relevanz für die Abschlussprüfung, aber auch datenschutzrechtliche Anforderungen oder soziale Anforderungen, wie die Einhaltung moralischer und ethischer Vorgaben, welche sich unter anderem im Code of Conduct des Auftraggebers niederschlagen können. Outsourcingverträge werden in der Praxis üblicherweise über eine längere



Dr. Michael Heym



Martin Seeburg

Laufzeit geschlossen. Fünf bis acht Jahre sind hier durchaus keine Seltenheit. Daher müssen sich wandelnde Anforderungen der Compliance soweit wie möglich bei der Auswahl des Auftragnehmers (im Rahmen des „Request for Proposal“-Prozesses) und der Vertragsgestaltung strukturell antizipiert werden. Für die Fälle, in denen dies nicht ausreicht, müssen laufende Vertragsbeziehungen im Rahmen der Vertrags-Governance angepasst werden. Die Compliance-Anforderungen an diesen Prozess sind ebenfalls nicht zu vernachlässigen, sollen hier aber nicht Gegenstand der Betrachtung sein.²

Üblicherweise werden im Outsourcing heutzutage serviceorientierte Verträge geschlossen. Das bedeutet, dass der Auftragnehmer seine Leistung entsprechend zuvor vereinbarter Rahmenbedingungen (Rahmenvertrag) sowie Leistungsbeschreibungen und Service-Level-Vereinbarungen (beides in den Leistungsverträgen bzw. Statements of Work) erbringt.

Der Auftraggeber behält dabei keinen oder nur einen sehr beschränkten Einfluss auf die Ausführung. Dies ist durchaus gewünscht, um beispielsweise Skaleneffekte durch die Plattformstrategie des Anbieters zu erzielen oder um divergierende Interessenlagen innerhalb der Organisation des Auftraggebers zu egalisieren. Interessanterweise resultieren letztere in der Praxis oft auch aus unterschiedlichen Compliance-Anforderungen der Landesgesellschaften und des Konzerns. Umso mehr erzwingt diese Managementform aber, Compliance-Anforderungen auf allen Vertragsebenen zu berücksichtigen.

2. Wesentliche Compliance-Anforderungen an Outsourcingverträge

In der Vertragshierarchie eines Outsourcingvertragswerks nimmt der Rahmenvertrag üblicherweise die ranghöchste Position ein. Im Rahmenvertrag oder dessen Anhängen werden bezüglich der Compliance üblicherweise die relevanten, klar definierten Anforderungen betreffend zu erfüllender Rechtsnormen,

* Dr. Michael Heym ist Gründungspartner und Miteigentümer der Navisco AG, Sourcing Professionals, und blickt auf eine über 15-jährige IT-Erfahrung in verschiedenen nationalen und internationalen Managementpositionen zurück. Kontakt: michael.heyman@navisco.com. Martin Seeburg leitet Projekte der Navisco AG, insbesondere zu Sourcing-Ausschreibungen und Sourcing-Strategien für international tätige Unternehmen und hat über zehn Jahre Erfahrung im internationalen Outsourcingumfeld. Kontakt: martin.seeburg@navisco.com.

1 Vgl. BITKOM (Hrsg.): Compliance in IT-Outsourcing Projekten, Berlin 2006, S. 18 und 41ff.

2 Vgl. Gottmann, H.: Betrugsrisiken im IT Outsourcing, in: ZRFC 3/2009, S. 140ff.

3 Vgl. Grummer, J.-M./Seeburg, J.: SOX und BilMoG Compliance, in: Behringer, S. (Hrsg.): Compliance kompakt, Berlin 2011, S. 150-152.

Standards, Code of Conducts sowie Good oder Best Practices vereinbart. Eine Auswahl von je nach Fall wichtigen Anforderungen zeigt untenstehende Tabelle. Außerdem werden die Orte des Leistungsbezugs in einem von den Vertragsparteien über die Laufzeit des Vertrags aktuell zu haltenden Anhang spezifiziert. Der Rahmenvertrag muss die sich hieraus ergebenden landesspezifischen Anforderungen möglichst generisch widerspiegeln, um offen für entsprechende Veränderungen beim Auftraggeber zu sein. So kann zum Beispiel die Einhaltung lokalen Rechts für die Archivierung von Geschäftsunterlagen vereinbart werden, wobei sich die Bedeutung von „lokal“ durch Änderungen

Anforderung	Zweck/ Inhalt
ISAE 3402, IDW PS 951, PS 890, SOC 1/SSAE 16 (ehemals SAS 70)	Vermeidung von Audits des Auftraggebers bzw. deren Wirtschaftsprüfern im Umfeld SOX/ 8. EU-Richtlinie (BilMoG in Deutschland) beim Auftragnehmer. Der ausgelagerte Bereich des IKS wird attestiert und kann dann als „Black Box“ akzeptiert werden.
ISO 27001	Qualität im Management der Informationssicherheit, international anerkannte Norm und zertifizierbar für Auftragnehmer (in Deutschland auch gemäß den Anforderungen nach BSI-Grundschutz)
ITIL	IT-Service-Management; als Good Practices quasi der Qualitäts-Benchmark
ISO 20000	Qualität im IT-Service-Management, international anerkannte und an ITIL ausgerichtete Norm, zertifizierbar für Auftragnehmer
ISO 9001	Grundlegende Norm im Qualitätsmanagement, international anerkannte Norm und zertifizierbar für Auftragnehmer
ISO 14001	Qualität im Umweltmanagement, international anerkannte Norm und zertifizierbar für Auftragnehmer
BS 25999	Good Practices zur Sicherstellung des Betriebs im Hinblick auf Risiken (Business Continuity), zertifizierbar für Auftragnehmer
COBIT	Qualität in der IT-Governance generell, international anerkanntes Framework
CMMI-DEV	Sammlung von Best Practices zur Qualitätssicherung der Softwareentwicklungs- und Wartungsprozesse, international anerkannte Norm und zertifizierbar für Auftragnehmer
Branchenstandards	Je nach Branche gilt es, spezifische Anforderungen zu erfüllen. Beispiele sind PCI DSS, MaRisk oder Basel II.
Unternehmensstandards	Je nach Unternehmen gilt es, die spezifischen Anforderungen aufzugreifen. Beispiele sind der Code of Conduct oder die Security-Richtlinien
Lokale Gesetze und Rechtsprechung	Je nachdem welche Länder vom IT-Outsourcing direkt oder indirekt betroffen sind, gilt es, die dortigen gesetzlichen Anforderungen zu erfüllen. Ein Beispiel ist die Aufbewahrungsfrist für Geschäftsunterlagen bei Archivierung und deren Unveränderbarkeit.

Tabelle: Auswahl von je nach Fall relevanten Compliance-Anforderungen für IT-Outsourcingverträge im deutschsprachigen Raum

der Orte des Leistungsbezugs über die Vertragslaufzeit wandelt.

Dem Rahmenvertrag nachrangig werden in Leistungsverträgen üblicherweise genaue Leistungsbeschreibungen und Service Level vereinbart. Hierbei gilt es, die Ausgestaltung der Anforderungen im Detail zu spezifizieren, ohne dass sich Widersprüche zum Rahmenvertrag ergeben. Wesentliche Inhalte sind hier die Verantwortlichkeiten und Mitwirkungspflichten von Auftraggeber und Auftragnehmer (soweit möglich aus Prozesssicht), Betriebs- und Servicezeiten, Key-Performance-Indikatoren (KPI) und Service-Level-Vereinbarungen (SLA) wie zum Beispiel die zugesicherte Verfügbarkeit einer Applikation sowie das Reporting. Die eigentliche Umsetzung und technische Realisierung innerhalb der gesetzten Parameter obliegt dem Auftragnehmer. Aus Sicht des Compliance-Beauftragten gibt es also klare, wohldefinierte Schnittstellen zwischen Auftraggeber und Auftragnehmer, welche üblicherweise individuell verhandelt werden. Nicht zuletzt deshalb ist die Einbeziehung des Compliance-Beauftragten in Ausschreibung und Verhandlungen geboten.

Natürlich könnte der Auftraggeber seine Compliance-Anforderungen schlicht maximieren, um auf der sicheren Seite zu sein. Dies ist jedoch üblicherweise die teuerste Option und da Kosteneinsparungen zumeist ein Antrieb für Outsourcingentscheidungen sind, auch in der Regel nicht gewollt.

Auch die grundsätzlichen Anforderungen des Auftraggebers zur Auditierbarkeit des Auftragnehmers sind im Vertragswerk festzuhalten. In vielen Fällen wird man sich zwar den eigentlichen Audit sparen wollen und dafür die Erbringung eines entsprechenden Zertifikats oder Attestes durch den Auftragnehmer einfordern, doch darf sich der Auftraggeber die Möglichkeit eines Audits – in Deutschland insbesondere auch im Kontext des Bilanzrechtsmodernisierungsgesetzes vom Mai 2009 (BilMoG) – nicht nehmen lassen.³ Ein Spezialfall in diesem Zusammenhang sind Unterstützungsleistungen des Auftragnehmers bei internem oder gerichtlich veranlasstem Informationsbedarf (beispielsweise zur Aufdeckung von Fraud). Auch hierfür sind entsprechende

Regelungen zu vereinbaren, was sich in der Verhandlungspraxis oft schwierig gestaltet, da wiederum die Compliance des Auftragnehmers tangiert sein kann.

Nicht zuletzt muss die Implementierung einer beiderseitigen Vertrags-Governance im Rahmenvertrag sichergestellt werden, so dass der Vertrag mittels Change-Management jederzeit geänderten Anforderungen bezüglich der Compliance des Auftraggebers angepasst werden kann.

3. Aktuelle Entwicklungen

3.1 ISAE 3402, SSAE 16 und SOC 1-3

Von aktueller Bedeutung sowohl für Neuals auch für Bestandsverträge (und damit auch ein gutes Beispiel für die Anforderungen an die Vertrags-Governance) ist das Inkrafttreten des International Standard on Assurance Engagements (ISAE) 3402 am 15. Juni 2011, für Geschäftsjahre, die an oder nach diesem Stichtag enden. Bis zu diesem Zeitpunkt gab es keinen internationalen Standard zur Bestätigung des Vorhandenseins oder der Funktionsfähigkeit des internen Kontrollsystems bei Auftragnehmern im IT-Outsourcing.⁴ Auch wenn SAS 70 in der Praxis de facto diese Rolle übernahm, sind beispielsweise in Deutschland der IDW PS 951 und in der Schweiz der PS 890 relevant. Da im Outsourcing aber häufig Ländergrenzen überschritten werden, wird der ISAE 3402 den Grad der Sicherheit erhöhen und sollte in Abhängigkeit der Anforderungen der jeweiligen Revisoren und Wirtschaftsprüfer in die Verträge aufgenommen werden.

In den USA löste entsprechend am 15. Juni 2011 der US-Standard SSAE 16 den Vorgänger SAS 70 ab, welcher damit in der Praxis ausläuft. Es ist zu beachten, dass es zwischen SSAE 16 und ISAE 3402 durchaus Unterschiede gibt, welche gegebenenfalls einer Bewertung bedürfen. Einer der Unterschiede besteht darin, dass ein SSAE-16-Report, der unter das SOC 1 Reporting Framework fällt, hinsichtlich des Nutzerkreises auf das Management des Dienstleisters sowie dessen Kunden und deren Wirtschaftsprüfer beschränkt ist. ISAE 3402 kennt hier keine Vorgaben, schließt Einschränkungen des Nutzerkreises aber auch nicht aus.⁵ ISAE-3402-Reports eignen sich daher prinzipiell auch für die Verwendung im Marketing und Vertrieb, so-

fern die attestierenden Unternehmen hierbei mitspielen. Auch in anderen Ländern wie Deutschland und der Schweiz haben lokale Standards nach wie vor Bestand. Eine vollständige Harmonisierung besteht daher bis dato also nicht. Ebenfalls offen ist, ob und welche Rolle die gleichfalls neuen SOC-2- und SOC-3-Reports für die Compliance bezüglich Sicherheit, Verfügbarkeit, Prozessintegrität und Vertraulichkeit spielen werden. SOC 2 wird als Typ I analog zu SOC 1 vereinfacht gesagt die Eignung der Kontrollen attestieren, während Typ II auch deren Effektivität einschließt. SOC 3 wird quasi die im Nutzerkreis uneingeschränkte und vereinfachte Fassung hiervon und dürfte somit zumindest für Marketing und Vertrieb von Anbietern Bekanntheit erlangen.⁶ Ihm könnte auch besondere Bedeutung im Cloud Computing zuwachsen. Insbesondere die möglichen Auswirkungen auf den deutschsprachigen Raum lassen sich aber derzeit noch nicht abschließend beurteilen.

3.2 Cloud Computing

Der Begriff Cloud Computing geistert schon seit einiger Zeit durch das Marketing der IT-Branche. Mittlerweile hat sich aber ein üblicherweise anerkanntes Verständnis hiervon etabliert. Man unterscheidet allgemein:⁷

- ▶ Software as a Service (SaaS)
Der Auftraggeber nutzt eine Software in einem externen Rechenzentrum. Die komplette Verantwortung für Betrieb, Wartung und Weiterentwicklung liegt beim Auftragnehmer. Der Auftraggeber hat maximal die Möglichkeit anwenderspezifischer Konfiguration.
- ▶ Platform as a Service (PaaS)
Der Auftraggeber behält gegenüber SaaS die Kontrolle über die Applikation und gegebenenfalls die Konfiguration der Betriebsumgebung.
- ▶ Infrastructure as a Service (IaaS)
Der Auftraggeber behält gegenüber SaaS die Kontrolle über die Applikation, Betriebssysteme, Speicher und gegebenenfalls die Konfiguration einzelner Netzwerkhardwarekomponenten.

Wirklich neu ist hier hinsichtlich der Technik oder der Leistung also nichts. Alle Varianten des Cloud Computing sind schon seit geraumer Zeit Bestandteil von Outsourcingverträgen. Man spricht hier auch von „Private Clouds“. Von neuer Bedeutung sind allerdings die sogenannten „Public Clouds“ – es gibt noch diverse Mischformen, welche hier aber nicht betrachtet werden sollen –, bei denen obige Services als Produkte von der Stange in den Markt gepusht werden und insbesondere nicht kundenindividuell auf dessen Bedürfnisse angepasst sind. Da dies weitgehend auch die Vertragswerke betrifft, ergibt sich eine beson-

4 Vgl. Gaskin, F.: Roll Over, SAS 70 It's time for ISAE 3402 and SSAE 16, in: Accountancy Ireland 10/2010, S. 12.

5 Vgl. Gaskin, F.: Roll Over, SAS 70 It's time for ISAE 3402 and SSAE 16, in: Accountancy Ireland 10/2010, S. 14.

6 Vgl. Singleton, T. W.: Understanding the New SOC Reports, in: ISACA Journal 2/2011.

7 Vgl. Mell, P./ Grance, T.: The NIST Definition of Cloud Computing, Special Publication 800-145, 09/2011.

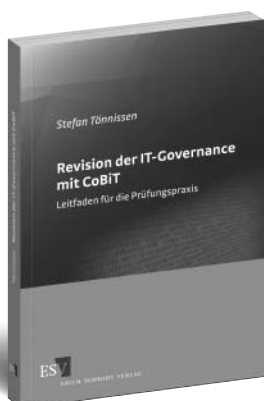
dere Compliance-Problematik für den Auftraggeber. Generell gibt es Services im Markt, welche bezüglich des einen oder anderen Standards zertifiziert sind (vgl. hierzu auch die Thematik SOC 3). Es besteht aber kein oder kaum Gestaltungsspielraum für den Auftraggeber. Ein besonderes Problem bei Public Clouds ist zudem der Ort der Datenverarbeitung und -speicherung, welcher im technisch optimalen Konzept einer Cloud undefiniert beziehungsweise jederzeit austauschbar bleibt, aufgrund möglicherweise divergierender Rechtssysteme für die Orte der Leistungserbringung aus Compliance-Sicht aber ein wesentlicher Parameter sein kann. Grundsätzlich kann man sagen, dass Verträge und Leistungen für Public Clouds entweder den Compliance-Bedarf des Auftraggebers erfüllen oder eben nicht. In letzterem Fall ist die Vermeidung eines Vertragsabschlusses die einzige Option. Bei bereits abgeschlossenen Verträgen wird im Fall veränderter Compliance-Anforderungen und deren Nichterfüllung durch den Vertrag dessen Kündigung folgen müssen. Aus diesem Grund ist bei der Nutzung von Public-Cloud-Services aus Compliance-Sicht eine kontinuierlich gepflegte Exit-Strategie geboten, um Compliance-Risiken vom Unternehmen abzuwenden.

4. Fazit

Beim IT-Outsourcing die Compliance des Auftraggebers zu erhalten ist keineswegs ein Selbstläufer. Die Einbeziehung des Compliance-Beauftragten in Ausschreibung und Vertragsverhandlungen oder Vertragsbewertung ist zwingend erforderlich, da die Vertragsgestaltung zunächst die einzige Stellschraube zur

Compliance im IT-Outsourcing ist. Während die Verantwortung beim Auftraggeber verbleibt, muss der Auftragnehmer die Anforderungen, die an den Auftraggeber gestellt werden, erfüllen. Der Auftraggeber hat aber keinen oder nur sehr beschränkten Einfluss auf die Leistungserbringung. Es gilt also alle Parameter des Vertrags richtig zu setzen. Im Fall von Public Clouds ist dies jedoch kaum möglich, denn Vertragsverhandlungen stehen dem Konzept einer Public Cloud entgegen.

Die Vertragslaufzeiten im Outsourcing sind üblicherweise lang genug, um mit Änderungen der Compliance-Anforderungen konfrontiert zu werden. Gerade sprachen wir noch von SAS 70, heute bereits von ISAE 3402. Nicht alle Änderungen lassen sich beim Vertragsentwurf antizipieren. Die Vertragspflege ist daher ein Thema für den Compliance-Beauftragten. ISAE 3402 sollte beispielsweise abhängig von den Anforderungen der jeweiligen Revisoren und Wirtschaftsprüfer in existierende Verträge mit aufgenommen werden, sofern bisher SAS 70 verwendet wurde.



Revision der IT-Governance mit CoBIT

Leitfaden für die Prüfungspraxis

Von Stefan Tönnissen

2011, 323 Seiten, mit zahlr. Beispielen und der Prüfungslandkarte IT-Governance, € (D) 49,95, ISBN 978-3-503-13012-2

Wirksame interne Kontrolle der IT

In der Praxis erschwert die Vielzahl unterschiedlicher Prüfungskataloge und spezifischer Richtlinien das so wichtige Prüfen und Bewerten der IT-Governance.

Auf Basis des internationalen Standards CoBIT bietet Stefan Tönnissen in diesem Buch einen Lösungsweg.

Aus der Praxis für die Praxis: Mit Beispiel-Prüfungsplan und Prüfungslandkarten!

Weitere Informationen:  www.ESV.info/978-3-503-13012-2



ERICH SCHMIDT VERLAG

Auf Wissen vertrauen

Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin ·

Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info