LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR INFORMATIK
LEHR- UND FORSCHUNGSEINHEIT
FÜR DATENBANKSYSTEME

Seminararbeit
in Informatik

IT-Outsourcing

Gesetzesrahmen und Compliance

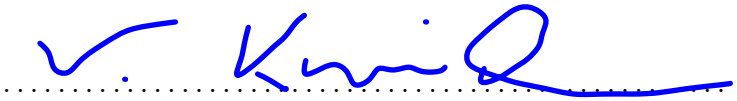
Verena Knerich

Aufgabensteller:	Dr. Frank Sarre
Betreuer:	Dr. Frank Sarre
Abgabedatum:	7. Dezember 2016

Erklärung

Hiermit versichere ich, dass ich diese Seminararbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 7. Dezember 2016



Verena Knerich

Zusammenfassung

Aufgrund verschiedener Faktoren wie dem zunehmendem Rationalisiserungsdruck, einer Fokussierung aufs Kerngeschäft und der Hoffnung auf einen kompetitiven Vorteil verlagern immer mehr Unternehmen ihre IT ins inner- oder außereuropäische Ausland. Dieser Outsourcing-Prozess beinhaltet jedoch nicht gleichermaßen eine Abschiebung der Verantwortung.

Um Strafmaßnahmen und Imageschäden vermeiden zu können, besteht die Notwendigkeit, sich mit einer Vielzahl von internationalen Gesetzgebungen auseinanderzusetzen (Compliance). Aufgrund der zugrunde liegenden Komplexität scheint Uneinigkeit darüber zu bestehen, wie weit Compliance im Kontext des IT-Outsourcing zu gehen hat.

Daher soll die vorliegende Arbeit eruieren, wie Compliance die Entscheidung für oder gegen IT-Outsourcing und dessen Durchführung beeinflusst, und welche Maßnahmen durch eine Befolgung notwendig werden können.

Dafür sollen die fraglichen Konzepte Compliance und Outsourcing definiert und ein grober Überblick über die relevanten gesetzlichen Rahmenbedingungen, Richtlinien, Zertifikate und Referenzmodelle gegeben werden. Darauf aufbauend werden Gründe für oder gegen IT-Outsourcing erörtert und mögliche Vorteile und Herausforderungen aufgezeigt.

Inhaltsverzeichnis

Kapitel 1

IT-Outsourcing als aktueller Trend

Laut aktuellen Statistiken der Computerwoche scheint der Umsatz in kommerziellen Outsourcing-Deals in Deutschland stetig zuzunehmen (Hülsbömer 2016). Dieser Trend speist sich unter anderem aus dem zunehmenden Konkurrenzdruck, dem Anspruch, sich aufs Kerngeschäft zu fokussieren, der einfacheren Vergleichbarkeit und der Hoffnung, sich gegenüber Konkurrenten einen Wettbewerbsvorteil zu sichern (Hodel u.a. 2006). Gerade die IT-Abteilungen oder auch IT-lastige Geschäftsprozesse werden häufig aus dem Unternehmen ausgelagert.

Mindestens in dem gleichen Maße wie Outsourcing selbst, nimmt jedoch auch die Anzahl und Komplexität der Gesetze und Regelungen zu, die es bei Outsourcing zu beachten gilt (Mossanen 2010). Dieses Gewebe zu überblicken, stellt für Unternehmen eine große Herausforderung dar; zumal wenn es gilt, Compliance-Anforderungen genügen zu wollen. Dieser Anspruch wiederum rechtfertigt sich durch das zunehmende Interesse der Öffentlichkeit, interne Strukturen von Unternehmen zu hinterfragen, sowie durch in den Medien publik gemachte Compliance-Untersuchungen (o.A. 2009).

Aufgrund der Aktualität und Vielschichtigkeit der Thematik soll die vorliegende Arbeit einen Einblick in die Zusammenhänge zwischen IT-Outsourcing und Compliance bieten. Zunächst werden dafür die relevanten Konstrukte definiert und ein Überblick über einige der Einfluss nehmenden gesetzlichen Rahmenbedingungen offeriert. Im dritten Kapitel findet sich ein Auszug zu Richtlinien, Zertifikaten und Referenzmodellen, die beim Outsourcing berücksichtigt werden können. Aufbauend auf den vorherigen Informationen dient das letzte Kapitel dazu, die Informationen zu bündeln und Argumente für und gegen Outsourcing unter Berücksichtigung von Compliance-Aspekten anzuführen.

Kapitel 2

Definitionen

In der Literatur finden sich teils widersprüchliche Definitionen zu Begriffen wie Outsourcing und Compliance. Deswegen soll an dieser Stelle für die vorliegende Arbeit klar dargestellt werden, welche Aspekte hier berücksichtigt werden.

2.1 IT-Outsourcing

Gemeinhin versteht man unter IT-Outsourcing die „mittel- bis langfristige Übertragung von wesentlichen, aber nicht zu den Kernkompetenzen zählenden Teilen der Informationstechnologie bzw. die Auslagerung von ganzen Geschäftsprozessen mit hohem IT-Anteil an einen spezialisierten, externen IT-Dienstleister, bei vorheriger Eigenerstellung der entsprechenden Leistung."' (Mossanen 2010).

Zentral an dieser Definition ist, dass der auszulagernde Teilbereich vorher vom Unternehmen selbst geleistet wurde und nun für einen festgelegten Zeitraum an Dritte übertragen wird. Bei diesem Teilbereich kann es sich einerseits um IT-Infrakstrukturkomponenten oder -anwendungen wie den Rechenzentren, dem Netzwerk oder transaktionale Anwendungen handeln (o.A. 2009. Es kann sich aber auch auf Prozesse wie die Buchhaltung und das Finanzwesen beziehen, bei denen besondere Umsicht bei der Prüfung der zu befolgenden Gesetze geübt werden sollte.

Abhängig von den betrachteten Eigenschaften, kann Outsourcing unterschiedlich klassifiziert werden. Eine der wichtigsten Merkmale bezieht sich auf den Ort relativ zum outsourcenden Unternehmen. Werden die Prozesse zwar ausgelagert, aber nach wie vor im Inland behandelt, so bezeichnet man dies als Onshoring. Nutzt man die naheliegenden Niedriglohnregionen Europas spricht man von Nearshoring während sich Offshoring auf weiter entfernt liegende, internationale Standorte bezieht (Knolmayer 2007).

Andere Klassifizierungen unterscheiden basierend auf dem Grad der externen Leistungsbeziehung, der finanziellen Abhängigkeit oder der Geschäfts-

orientierung. Ersteres bezieht sich darauf, wie viele Teile des Unternehmens ausgelagert werden, worauf basierend man von totalem oder selektivem Outsourcing spricht. Bei der finanziellen Abhängigkeit ist der Umfang der Verantwortungsübertragung an die externen Partner von Bedeutung. Der Grad der Geschäftsorientierung knüpft an die vorweg erwähnten Unterarten derjenigen Teile des Unternehmens an, die verlagert werden. Je nach Art des ausgelagerten Prozesses, wird das Outsourcing selbst unterschiedlich bezeichnet. Für eine ganzheitliche Darstellung der möglichen Bezeichnungen siehe Grafik 2.1

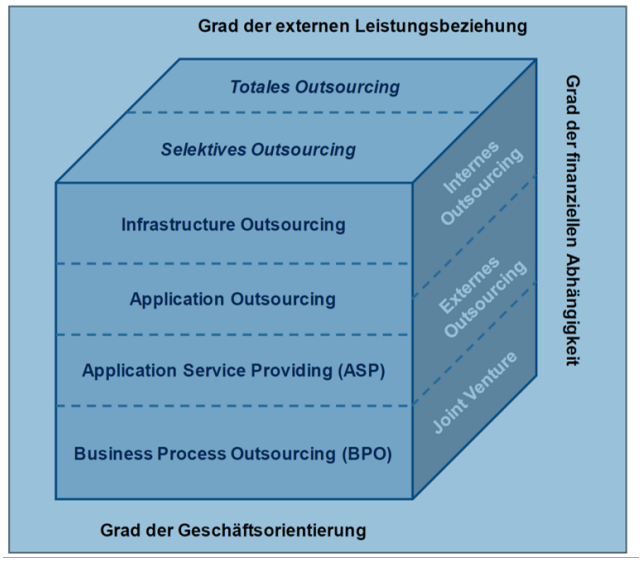


Abbildung 2.1: Mögliche Charakterisierung von Outsourcing (o.A. 2009)

2.2 Compliance

Unter Compliance versteht man die „unternehmensweite und -übergreifende Anstrengung mit der Zielsetzung, externe sowie interne Vorschriften und Vorgaben unter der konsistenten Berücksichtigung von existenten und potentiellen Risiken einzuhalten“ (Mossanen 2010). Diese Vorschriften und Vorgaben, die es einzuhalten gilt, können gerade im Bereich des IT-Outsourcing relativ schwer zu überblicken sein. Die Einhaltung derselbigen ist also primär eine Managementaufgabe und wird gemeinhin beim Outsourcing auch nicht an die externen Partner abgetreten (s. Kapitel **??**).

Bei angemessener Befolgung führt Compliance zu besserer Transparenz und Kontrolle innerhalb eines Unternehmens, zu einer Erhöhung der IT-Qualität und - Sicherheit und hilft dank der engen Anbindung an ein umfassenden

Risiko-Management potentielle Risiken zu minimieren (Klotz 2009). Je nach Kontext, können Verstöße mit Haftstrafen, Geldbußen, Hausdurchsuchungen, zivilrechtlichen und Schadenersatzansprüchen, steuerlichen Folgen, negativem Ranking oder (inter-)nationalen Sperren geahndet werden. Problematisch bleibt jedoch, dass unter Umständen bis zu 10.000 Vorschriften berücksichtigt werden müssen (o.A. 2009).

Bereiche, die von Compliance normalerweise betroffen sind, umfassen von der Einführung eines Informations- und Kontrollsystems (IKS), über die Berücksichtigung von Datenschutz, Datensicherheitsvorgaben und IT-Security bis hin zur zur Archivierung und Kontrolle der IT-Nutzung durch die Mitarbeiter sämtliche Unternehmensbereiche (Mossanen 2010, Rath 2008).

Missverständlich ist in diesem Kontext häufig der Unterschied zwischen IT-Compliance und IT-gestützter Compliance. Bei ersterem handelt es sich um Regel-konformes Verhalten in Bezug auf die IT, bei letzterem wird die Konformität erst durch Nutzung der IT erreicht (Mossanen 2010, Klotz 2009).

Kapitel 3

Gesetzliche Rahmenbedingungen

Wie im Vorangegangen immer wieder angesprochen wurde, gilt es gerade beim IT-Outsourcing eine Vielzahl an gesetzlichen Regelungen zu überblicken. Zum Teil ergibt sich diese Komplexität aus den Verflechtungen zwischen unterschiedlichen Formen seien es Gesetze, Richtlinien oder Standards, was Einfluss auf die Notwendigkeit ihrer Einhaltung mit sich bringt. Um mögliche Verständnisschwierigkeiten zu vermeiden, soll daher im Folgenden zunächst kurz erklärt werden, wo die Unterschiede liegen.

3.1 Arten von Rechtsquellen

Der vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) herausgegebene Leitfaden unterscheidet unter anderem zwischen folgenden Arten von Rechtsquellen: formelle Gesetze, Gesetze im materiellen Sinn, Richtlinien und Standards (Weber 2006).

Beide Arten von Gesetzen haben gemein, dass sie abstrakt gehalten sind und auf ein Ziel hinwirken. Während formelle Gesetze wie das Europäische Primärrecht und nationale Gesetze durch ein parlamentarisches Verfahren zustande gekommen sind, müssen materielle Gesetze aufgrund einer Ermächtigungsnorm von der Verwaltung erst erlassen werden. Ein Beispiel hierfür wäre die Telekommunikationskundenschutzverordnung (2006).

Richtlinien dagegen werden von der Verwaltung herausgegeben und legen bestehende Gesetze aus, konkretisieren sie und spiegeln somit die Rechtsauffassung der Verwaltung in bestimmten Fällen wieder. Sie haben keinen Rechtscharakter im eigentlichen Sinne, können aber dennoch bindend sein, wenn sie von internationalen Organisationen veröffentlicht und fixiert wurden (o.A. 2009).

Wie der Name nahe legt, handelt es sich bei einem Standard um eine Vereinheitlichung, die sich etabliert hat. Auch hier fehlt der eigentliche Rechtscharakter, es sei denn sie sind Bestandteil einer Prüfung oder eines Regelwerks (2009). Diese werden häufig privatrechtlich ausgehandelt und unterliegen der Selbstverpflichtung (Weber 2006).

Hinzu kommen die Referenzmodelle, welche eher der Orientierung denn den konkreten, rechtsfähigen Vorgaben dienen. Anhand ihres Musters können entweder spezialisierte Vorgehensweisen abgeleitet werden oder der Vergleich mit anderen Modellen wird ermöglicht (o.A. 2009).

Mit Zertifikaten, die Weber ebenfalls den Standards zuordnet (2006), können über Kontrollmaßnahmen und Tests ein eingehaltener Standard, ein Referenzmodell oder eine Richtlinie nachgewiesen werden. Dies dient zumeist dafür, der Öffentlichkeit ein positives Bild über das eigene Unternehmen zu vermitteln (o.A. 2009).

3.2 Eine Auswahl relevanter Verfügungen

Betrachtet man eine der Primärquellen zu den gesetzlichen Rahmenbedingungen, den BITKOM Leitfaden, wird man mit einer Vielzahl an zu beachtenden Regelungen konfrontiert. Aufgrund des vorgegebenen Umfangs soll in dieser Arbeit nur eine Auswahl angeführt und weitere Fragen an den Leitfaden weiter delegiert werden (Weber 2006).

Wichtig bei (fast) allen Regelungen ist, dass der Outsourcing-Auftraggeber im Normalfall durch Delegation der Aufgaben an Outsourcing-Partner nicht von seiner Verantwortung entbunden wird. Verlagerung der Aufgaben heißt nicht Verlagerung der Verantwortung!

Zunächst sei das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) genannt. Es fordert die unternehmensweite Einführung eines Risiko-Management Systems und eines Informations- und Kontrollsystems (IKS) (Rath 2007); auch von Outsourcing-Partnern. Wie vorher erwähnt, ist der Auftraggeber in der Pflicht, die Einführung auch bei etwaigen Partnern zu gewährleisten. Im Rahmen einer jährlichen Überprüfung wird das System auf Inhalt und Aussagekraft überprüft (Weber 2006).

Laut dem BITKOM Leitfaden spielen auch GmbH Gesetze und das HGB bei IT-Outsourcing eine zentrale Rolle. Dies liegt unter anderem daran, dass das GmbH Gesetz die Einhaltung der Sorgfaltspflicht und der Ordnungsmäßigkeit der Buchführung einfordert. Welchen genauen Anforderungen dies zu genügen hat, wird wiederum in den Grundsätzen ordnungsgemäßer Buchführung (GoB) spezifiziert, bei denen es sich rein formell um Richtlinien und nicht prinzipiell um Gesetze handelt. Sie beinhalten die folgenden Prinzipien:Übersichtlichkeit,

Vollständigkeit, Ordnung, Zeitgerechtheit, Nachprüfbarkeit, Richtigkeit und die Einhaltung von Aufbewahrungsvorschriften (2006). Die Einhaltung dieser Richtlinien nimmt im IT-Bereich eine Sonderrolle ein, da in diesem Kontext auch Fragen der Datensicherheit und Nachvollziehbarkeit eine Rolle spielen. So ist zu berücksichtigen, dass etwa ein Wechsel des EDV-Systems die Daten nicht beeinträchtigen darf und unberechtigter Zugriff unbedingt vermieden werden muss - gleichgültig, ob es sich um das eigentliche Unternehmen oder Outsourcing-Partner handelt (Rath 2007).

Das zentrale Thema Datensicherheit wird vom Bundesdatenschutzgesetz (BDSG) geregelt. Mit dessen Anpassung an die EU-Richtlinien im Jahre 2002 wird erneut die enge Verknüpfung von Richtlinien und Gesetzen deutlich. Es fordert, dass personenbezogene Daten nur dann erhoben, verarbeitet und genutzt werden dürfen, sofern dies gesetzlich explizit erlaubt ist oder die Einwilligung der Betroffenen vorliegt. Unter personenbezogenen Daten sind in diesem Kontext alle sachlichen oder persönlichen Angaben zu den Verhältnissen ein Person zu verstehen. Allgemein gilt grundsätzliches Übermittlungsverbot, eine Prüfung kann im Einzelfall erfolgen (Weber 2006).

Je nach Art der Aufgabenübertragung an Outsourcing-Partner kann hier ein Fall eintreten, bei dem der Auftraggeber die Verantwortung an Dritte weitergibt. Sofern es sich um eine Funktionsübertragung handelt, sprich der Outsourcing-Partner übernimmt Datenverarbeitungsvorgänge samt der zugrunde liegende Aufgaben, so ist der Auftraggeber von der Verantwortung für den Schutz dieser Daten entbunden. Nichtsdestotrotz verbleibt ihm die Pflicht, seine Vertragspartner sorgfältig auszuwählen (o.A. 2009).

Der Sarbanes-Oxley-Act (SOX/SOA/SarbOx) wurde 2002 zwar in den USA erlassen, gilt allerdings auch für deutsche Unternehmen, da er sich auf alle Unternehmen deren Wertpapiere in den USA gehandelt werden, bezieht. Es nimmt sämtliche Outsourcing-Partner in die Pflicht, ein jährlich zu überprüfendes IKS zu schaffen. In einer zusätzlichen Publikation des Public Companies Accounting Oversight Board (PCAOB) wird erneut explizit darauf hingewiesen, dass eine Auslagerung von Aufgaben nicht nicht die Auslagerung der Verantwortung umfasst (Hall, Liedtka 2007).

Kapitel 4

Richtlinien, Zertifikate und Referenzmodelle

Wie im Kapitel 3.1 bereits erklärt wurde, stellen weder Richtlinien, Zertifikate noch Referenzmodelle gemeinhin rechtsgültige Vorgaben dar, jedoch können durch ihre Verflechtungen mit anderen Rechtsformen und den Übergang in best practice Ansätze ihre Einhaltung von großer Bedeutung sein.

4.1 Zwei etablierte Richtlinien

Mögliche Beispiele für relevante Richtlinien sind die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), welche offensichtlich in der IT-Branche höchst relevant sind. Sie legen fest, dass Finanzbehörde bei steuerlichen Außenprüfungen über das Recht verfügt, auf steuerrelevante Daten zuzugreifen. In Anlehnung an die GoB fordern sie, dass die steuerrelevanten Daten identifiziert, vollständig und unverändert archiviert und unveränderbar gespeichert zu sein haben. Erneut sieht man den engen Zusammenhang zu Themen wie IT-Sicherheit, Datenschutz und Datensicherheit. Ihre rechtliche Grundlage fußt primär auf den den §§ 146 Abs. 5, 147 Abs. 6 Abgabenordnung (AO) (Weber 2006).

Im Rahmen der Baseler Eigenkapitalvereinbarung (Basel II) müssen Banken Risiken von Unternehmen per Rating ermitteln. Dies spielt insbesondere im Kontext des Risiko-Managements eine Rolle, da im Falle der Bewertung als unzureichend mit höheren Kreditzinsen oder höheren Sicherheiten zu rechnen ist(2006). Im Umkehrschluss bedeutet dies, dass detaillierte interne Kontrollanforderungen eingehalten werden müssen - zumal IT-Systeme als besonders anfällig gewertet werden. Zudem ist zu berücksichtigen, dass die Unternehmen potentielle Outsourcing-Partner in dieser Hinsicht sehr gewissenhaft prüfen sollten (o.A. 2009).

4.2 Zertifizierungen als Beispiele für Standards

Standards im Allgemeinen sind ähnlich zu Vereinheitlichungen, die sich durchgesetzt haben. Dazu zählen, wie bereits erwähnt, die Grundsätze ordnungsgemäßer Buchführung oder die Wirtschaftsprüfungsstandards. Da diese eine Sammlung der Regeln zur Berufsausübung beinhalten und nicht speziell auf den IT-Bereich ausgerichtet sind, sollen sie hier nicht weitere Beachtung finden (für weitere Informationen o.A. 2009).

Zertifizierungen können jedoch ebenfalls als Standards angesehen werden. Sie bieten zusätzlich die Möglichkeit, die Einhaltung von Standards, Richtlinien etc. zu bescheinigen und dadurch zum Image des Unternehmens positiv beizutragen.

Ein prominentes Beispiel ist das Statement of Auditing Standards (SAS) 70 des American Insitute for Certified Public Accountants (AICPA). Er umfasst zwei Arten von Reports, Type I und Type II, die sich hinsichtlich ihrer Prüfbarkeit unterscheiden.

Anders als Type II bescheinigt Type I lediglich die Existenz eines IKS, macht aber keine Aussagen über den Test von Kontrollmaßnahmen. Type II kann herangezogen werden, um Compliance nachzuweisen. Dies kann über eine Vielzahl von Tests erreicht werden, die über einen längeren Zeitraum hinweg durchgeführt werden und die Effektivität sowie Wirksamkeit der internen Kontrollen abprüft. Zudem enthält es eine Beschreibung des IKS (Weber 2006). Ein nennenswerter Vorteil dieses Vorgehens ist, dass es lediglich einmal pro Outsourcing-Standort durchgeführt werden muss und dann auf andere übertragen werden kann. Als formalisierte Maßnahme kann er die Einhaltung der SOX-Vorschriften abprüfen. Das deutsche Gegenstück stellt meist die „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“ (IDW PS 331) (o.a. 2009). Wichtig ist, dass sowohl bei IDW PS 331 als auch SAS 70 keine genauen Angaben enthalten sind, welche Bestandteile des Kontrollsystems zu prüfen, sind sondern lediglich Vorgaben wie die Prozesse beurteilt werden. Im Speziellen obliegt die Spezifizierung der Inhalte den betroffenen Kunden und Prüfern (Weber 2006).

Das „IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik“ (BSI) ist im Kontext der IT-Sicherheit nützlich, da es bei der Identifizierung des aktuellen Stands der Techniks behilflich ist. Dadurch kann die Einhaltung eines geforderten Sicherheitsstandards einfacher gewährleistet werden (2006).

Ähnlich dienen ISO, DIN und ICE-Normen dazu, als Hilfsmittel und Anleitungen für das Qualitäts-Management zu fungieren. Aufgrund der Fülle an Möglichkeiten, sei an dieser Stelle nur noch der ISO 17799 Standard genannt, der ebenfalls Maßnahmen zur Herstellung von IT-Sicherheit enthält.

4.3 Beispiele für Referenzmodelle

Ein Referenzmodell ist ein allgemeines Modell für eine Klasse von Sachverhalten und kann als Vergleichsobjekt oder als Basis zur Entwicklung spezieller Modelle dienen.

Bekannte Beispiele sind COSO, CoBIT, ITIL, wobei laut BITKOM die beiden letzteren für den IT-Bereich als relevanter einzustufen sind (Weber 2006).

Das Referenzmodell „Control Objectives for Information and Related Technology“ (CoBIT) der „Information Systems Audit Control Foundation“ (ISACF) wurde bereits 1996 geschaffen und dient als international anwendbares Rahmenmodell. Durch die „CoBIT Control Objectives“ wird es möglich, die in einem IT-Kontrollsystem zu erreichenden Kontrollziele klar zu definieren und abzuprüfen. Empfehlenswert ist es, diese Vorgehensweise bei Auftraggebern und Outsourcing-Partnern gleichermaßen einzuhalten (2006).

Als Best Practice Ansatz ist die „IT Infrastructure Library“ (ITIL) am meisten verbreitet. Obwohl es nicht geeignet ist, um die Einhaltung der SOX-Vorgaben zu gewährleisten, so bietet es doch ein umfangreiches Anwendungsspektrum. Es ist an den typischen Lebenszyklus von IT-Leistungen angepasst, bietet Möglichkeiten um Risiken besser einschätzen zu können und schafft eine Basis für IT-Sicherheit. Durch die Verwendung von ITIL können Prozesse zwischen den verschiedenen Partnern leichter abgestimmt werden, da diese standardisiert werden (o.A. 2009).

Kapitel 5

Diskussion: IT-Outsourcing unter Compliance-Aspekten

Die bloße Anzahl und wechselseitige Abhängigkeit der bisher vorgestellten Hintergründe, Gesetze, Richtlinien und Standards legt nahe, dass IT-Outsourcing ein vielschichtiges Thema ist, bei dem das Für und Wider sorgsam abgewogen werden muss. Dieser Umstand wird noch erschwert, wenn man strenge Compliance-Anforderungen anlegt. Zu welchen Argumenten dieses Zusammenspiel führt, soll im Folgenden erörtert werden.

5.1 Argumente für Outsourcing

Als einer der wichtigsten Gründe für IT-Outsourcing wird zumeist die erhoffte Kostenersparnis angeführt. Dies basiert einerseits auf der Kostenreduktion, da beispielsweise Personalkosten in Niedriglohnländern geringer ausfallen. Durch die Fokussierung auf das eigentliche Kerngeschäfft im Hauptunternehmen kann zudem angestrebt werden, Ressourcen effizienter zu nutzen (Yang, Huang 2000). Der zunehmende Wettbewerbsdruck im Inland und der daraus resultierende Rationalisiserungsdruck sollte einen weiteren Faktor darstellen, die Kosten für Standardleistungen so gering wie möglich zu halten (o.A. 2009).

Dieses Streben kann außerdem dadurch gerechtfertigt werden, dass die Leistungen des Kerngeschäfts schwerer imitierbar sind und den eigentlichen Kundennutzen beinhalten. Zudem behält sich ein Unternehmen so einfacher Flexibilität vor und kann agiler auf Änderungen reagieren. Im Allgemeinen können so auch die Time-to-Market Zyklen verkürzt werden. Neben dem finanziellen Vorteil, spielen also auch strategische Überlegungen eine Rolle (2009).

Neben der Optimierung von Kosten kann auch die Leistung als solches optimiert werden. Indem die bestmöglichen Partner für Dienstleistungen ausgewählt werden, kann ein hoher Qualitätsstandard erzielt und der Zugang zu

„state of the art“- Ausrüstung garantiert werden. Durch die erzwungene sehr detallierte Auseinandersetzung mit der eigenen Unternehmensstruktur bietet sich zudem die Möglichkeit, überholte Prozesse zu optimieren (2009).

5.2 Argumente gegen Outsourcing

Den vorherigen Argumenten kann man entgegen halten, dass die angestrebte Kostenersparnis geringer ausfallen könnte, als erwünscht. Dies hängt einerseits mit einer Unterschätzung der zugrunde liegenden Komplexität zusammen, was zu Mehrkosten bei der Einführungsphase führt und zudem weitgehende Anpassungen der eigenen Struktur mit sich bringen kann (o.A. 2009).

Ein weiterer wichtiger Faktor ist, dass sich Unternehmen potenziell von ihren Outsourcing-Partnern abhängig machen, zumal Änderungen nur langfristig erzielt werden können. Dies kann gegebenenfalls von Partnern ausgenutzt werden.

Konträr zu schnellen Time-to-market Zyklen kann Outsourcing auch mit einem Verlust des Innovationspotenzials einhergehen. Diese Gefahr besteht insbesondere, wenn hoch spezialisierte Prozesse ausgelagert werden und somit das Know-How nach Extern transferiert wird. Dabei gilt außerdem zu beachten, dass die eigenen Outsourcing-Partner möglicherweise auch anderen Kunden zur Verfügung stehen, was den angestrebten Wettbewerbsvorteil erheblich schmälert.

Ein Verlust des Know-How kann auch drohen, sollten Mitarbeiter, v.a. Spezialisten, das Vertrauen ins eigenen Unternehmen verlieren. Diese Vertrauenseinbußen können eine Begleiterscheinung von IT-Outsourcing sein, da das Betriebsklima potenziell als negativer wahrgenommen wird und Mitarbeiter um die eigene Stelle fürchten können. Solche Existenzängste beeinträchtigen fraglos die Produktivität, Motivation und emotionale Bindung ans Unternehmen, was zu weiteren Problemen führen kann (o.A. 2009). Aktuelle Schlagzeilen dienen bisweilen als Zeugnis dieser Vorgänge (z.B. o.A. 2016).

Kapitel 6

Fazit und Ausblick

Das Hauptaugenmerk der vorliegenden Arbeit lag auf der Darstellung wichtiger gesetzlicher Regelungen und Richtlinien zum Thema IT-Outsourcing und Compliance. Dabei sollte primär eruiert werden, welche Auswirkungen diese unter Berücksichtigung von Compliance auf IT-Outsourcing haben und welche Gründe demgemäß für und gegen IT-Outsourcing sprechen.

Die Ausführungen wurden auf den Definitionen von (IT)-Outsourcing und Compliance aufgebaut, um so das Problemfeld besser eingrenzen zu können. Dabei wurde deutlich, dass Outsourcing je nach Kontext sehr unterschiedlich definiert werden und Compliance Auswirkung auf sämtliche Unternehmensbereiche nehmen kann. Eine Sonderrolle nahm dabei das Risiko-Management ein.

Primär basierend auf dem Leitfaden der BITKOM wurden einige der wichtigsten gesetzlichen Regelungen dargestellt. Zum besseren Verständnis der Zusammenhänge wurde zunächst erklärt, bei welchen Vorschriften es sich um gesetzlich verpflichtende Vorgaben oder etablierte Best-Practice-Ansätzen handelt. Es wurde deutlich, dass eine Einhaltung sämtlicher Vorgaben ein großes Spektrum an Kontrollmechanismen nötig macht.

Es hat sich erwiesen, dass die Verwendung von Zertifizierungen und Referenzmodellen einen Teil dieser Komplexität durch Standardisierung abbauen kann. Dabei muss jedoch umsichtig geprüft werden, welche Vorgaben durch die Zertifikate und Referenzmodelle abgedeckt werden, und welche außen vor gelassen werden.

Der Überblick über die Rahmenbedingungen und sonstigen Richtlinien gipfelte in einer Diskussion der tatsächlichen pro und contra Argumente zum IT-Outsourcing. Es zeigte sich, dass obwohl Kostenersparnis als einer der Hauptgründe dafür gehandelt wird, die Sachlage dennoch differenzierter untersucht werden muss. So kann es durch Fehleinschätzungen oder dem Verlust von Innovativität letztlich zu weit weniger Erparnis kommen, als zunächst angenom-

men.

Basieren auf den Ahndungen bei Verstößen, potenziell schlechter Medienpräsenz und der Unübersichtlichkeit der Thematik ist davon auszugehen, dass Compliance auch zukünftig im Bereich IT-Outsourcing von entscheidender Bedeutung sein wird und eventuell sogar an Bedeutung gewinnen wird. Dies begründet sich unter anderem dadurch, dass durch einen unternehmensweiten Umgang mit Compliance nicht nur potenzielle Risiken minimiert werden können. In einer Zeit, in der die Verbrauchermeinung auch zu unternehmensinternen Vorgängen immer wichtiger wird, ist das Einhalten von Regelungen und ein umsichtiges Vorgehen nicht zu vernachlässigen. Berücksichtigt man diese Hintergründe bleibt abzuwarten, inwieweit IT-Outsourcing zukünftig praktiziert wird und wie damit umgegangen wird.

Abbildungsverzeichnis

Literaturverzeichnis

Hall, J., Liedtka, S. 2007. The Sarbanes-Oxley Act: Implications for Large Scale IT-Outsourcing. In: *Communications of the ACM*, Vol. 50, No. 3.

Hodel, M., A. Berger und P. Risi. 2006. *Outsourcing realisieren: Vorgehen für IT und Geschäftsprozesse zur nachhaltigen Steigerung des Unternehmenserfolgs*. Wiesbaden: Friedr. Vieweg & Sohn Verlag.

Hülsbömer, S. 2016. Die IT-Welt in Zahlen. *Coputerwoche von IDG*. http://www.computerwoche.de/a/die-it-welt-in-zahlen,2520525 [letzter Zugriff 7. Dezember 2016].

Klotz, M. 2009. *It-Compliance: Ein Überblick*. Heidelberg: dpunkt.

Knolmayer, G. 2007. Compliance Nachweise bei Outsourcing von IT-Aufgaben. In: *Wirtschaftsinformatik*, 49 (Sonderheft), S. 98-106.

Mossanen, K, J. Panitz und M. Amberg. 2010. *Compliance im IT-Outsourcing: Ermittlung von Einflussfaktoren und Entwicklung von Gestaltungsempfehlungen*. MKWI2010.

o.A. 2016. IT workers rally against offshore labor. In: *Computerworld*. http://www.computerworld.com/video/71975/it-workers-rally-against -offshore-labor [letzter Zugriff 7. Dezember 2016].

o.A. 2009. *Compliance im IT-Outsourcing: Theoretische und empirische Ermittlung von Einfluss-nehmenden Compliance-Faktoren*. http://wi3.fau.de/sites/default/files/projekte/Compliance_ im_ IT-Outsourcing_ -_ 20090216_ final.pdf [letzter Zugriff 7. Dezember 2016].

Rath, M. 2007. *Rechtliche Aspekte von IT-Compliance*. http://dsri.de/downloads/itc2007/folien/01-Rath.pdf [letzter Zugriff 7. Dezember 2016].

Rath, M. und C. Hunecke. 2008. Information Technology und Intellectual Property (IT/IP). In: *Corporate Compliance Checklisten*.Umnuß, K., Hg. 201-220. München: Beck.

Weber, M. 2006. *Compliance in IT-Outsourcing-Projekten: Leitfaden zur Um-*

setzung rechtlicher Rahmenbedingungen. Berlin: BITKOM.

Yang, C. und J. Huang. 2000. A decision model for IT-outsourcing. In: *International Journal of Information Management*. 20: 225-239.