Compliance im IT-Outsourcing

Ermittlung von Einflussfaktoren und Entwicklung von Gestaltungsempfehlungen

Kian Mossanen, Johannes C. Panitz, Michael Amberg

Lehrstuhl für Wirtschaftsinformatik III,
Friedrich-Alexander-Universität Erlangen-Nürnberg

1 Abstract

Dieser Artikel analysiert den Einfluss von Compliance auf das IT-Outsourcing und gibt Gestaltungsempfehlungen, wie dieser in IT-Outsourcing-Entscheidungsmodellen berücksichtigt werden kann. Die Ausführungen verstehen sich handlungsleitend für eine pragmatische Organisation von Compliance im IT-Outsourcing.

Das explorative Vorgehen ist auf qualitative und quantitative empirische Erhebungen gestützt und mündet in einem Bezugsrahmen. Dieser bildet durch die Angabe von Zielgrößen, Bedingungen und Aktionsparametern eine Gestaltungsgrundlage für die Berücksichtigung von Compliance im IT-Outsourcing.

2 Einführung

Die Anzahl und Komplexität von Gesetzen und Regelungen nimmt kontinuierlich zu. Viele Unternehmen sehen sich mit einer kaum mehr zu überblickenden Zahl an Vorgaben konfrontiert (Kley 2008, S. 14).[1] Unternehmensleitungen stehen vor der großen Herausforderung festzustellen, welche internen und externen Compliance-Anforderungen für ihr Unternehmen oder ihre aktuelle Entscheidungssituation Anwendung finden und wie diese erfüllt werden können.

Gerade die IT nimmt einen hohen Stellenwert bei der Gewährleistung von Compliance ein (Böhm 2008, S. 17). „Corporate Governance und Corporate Compliance sind angesichts der stetig zunehmenden Komplexität von Geschäfts-

[1] Die Rechtfertigung für dieses Vorgehen seitens der Behörden liefern die kapitalvernichtenden Unternehmensskandale in den USA und in Europa, aber auch der teilweise unverantwortliche Umgang mit vertraulichen Informationen (Kley 2008, S. 4).

prozessen in einem Unternehmen ohne den Einsatz von Informationstechnologie (IT) nicht mehr vorstellbar“ (Rath und Hunecke 2008, S. 201). Dies gilt für die Compliance von Prozessen, die im Unternehmen selbst stattfindenden, aber auch für ausgelagerte Bereiche (BITKOM 2006, S. 18). Bei der Berücksichtigung von Compliance im IT-Outsourcing ergeben sich daher folgende Problemfelder, die untersucht werden müssen:

- Identifikation und Interpretation der relevanten Compliance-Anforderungen im IT-Outsourcing
- Die Klärung der Zuständigkeit und Verantwortung von Compliance für ausgelagerte IT-Leistungen
- Umsetzung von Compliance im IT-Outsourcing.

Die Autoren haben im Rahmen ihrer Forschung erkannt, dass weder die wissenschaftliche noch die praxisorientierte Betrachtung des Themas „IT-Outsourcing unter spezieller Berücksichtigung von Compliance“ ausreichend erfolgt sind. Ein systematischer Ansatz, gegründet auf ein exploratives Vorgehen, zur Zusammenführung der Themen Compliance und IT-Outsourcing lässt sich in der Literatur nicht finden. Daher setzt dieser Artikel an der Erforschung dieser Problemstellung an und zeigt Lösungsansätze auf.

2.1 IT-Compliance

Compliance manifestiert sich in einer Reihe unterschiedlicher Begriffsdefinitionen. Aufgrund der Tatsache, dass sich die neuerliche Compliance-Diskussion noch im Anfangsstadium ihrer Entwicklung befindet, hat sich noch keine einheitliche Definition durchgesetzt. Infolgedessen findet die Anwendung des Begriffs in inkonsistenter Art und Weise statt (Hauschka 2008, S. VII; Kampffmeyer 2007, S. 3; Klotz und Dorn 2008, S. 7). Somit besteht die Notwendigkeit, ein leistungsfähiges Begriffssystem zu entwickeln, das die Verwertbarkeit und Austauschbarkeit von Erkenntnissen gewährleistet. Dieser Artikel folgt der nachfolgenden, hierfür entwickelten Compliance-Definition:

> Compliance ist eine unternehmensweite und -übergreifende Anstrengung mit der Zielsetzung, externe sowie interne Vorschriften und Vorgaben unter der konsistenten Berücksichtigung von existenten und potentiellen Risiken einzuhalten.

Die explizite Benennung der internen Vorgaben ist deshalb wichtig, da auch Verstöße gegen interne Vorgaben einen Verstoß gegen geltendes Recht darstellen können. Die Dynamik und Kontinuität von Compliance werden anhand der Nen-

nung von potentiellen Risiken ausgedrückt, wodurch auch die starke Verknüpfung mit dem Risikomanagement betont wird.[2]

Bei der *IT-Compliance* bezieht sich die Einhaltung von externen sowie internen Vorschriften und Vorgaben auf den Umgang mit der im Unternehmen vorhandenen IT. Daher versteht Klotz (2007a, S. 14) unter der IT-Compliance eine vorgabengerechte Gestaltung und einen regelkonformen Betrieb der IT.

Die IT-Compliance ist ein immaterieller Zustand, bei dem überprüft wird, ob die IT-Systeme die technischen, organisatorischen oder personellen Vorgaben erfüllen (Klotz und Dorn 2008, S. 6). „IT-Compliance reicht dabei von der Etablierung eines (am besten IT-gestützten) Informations- und Kontrollsystems (IKS) über die Einhaltung von Datenschutz und Datensicherheit sowie die Sicherstellung von „IT-Sicherheit" („IT-Security") bis hin zur gesetzeskonformen elektronischen Archivierung und Kontrolle der IT-Nutzung der Mitarbeiter" (Rath und Hunecke 2008, S. 201).

Gegen die IT-Compliance kann die IT-gestützte Compliance abgegrenzt werden. Die IT-gestützte Compliance bezeichnet die Gewährleistung von Compliance mit der Hilfe von IT (z.B. Beschaffungssysteme mit „Vier-Augen-Prinzip"[3], IT-gestützte Überprüfung von Genehmigungsprozessen) (Klotz und Dorn 2008, S. 9). IT-Compliance, das sind die Anforderungen an die IT selbst, während IT-gestützte Compliance die Herstellung von Compliance mit der Hilfe von IT umreißt.

2.2 IT-Outsourcing

Eine einheitliche begriffliche Definition ist im IT-Outsourcing nicht gegeben, da der Terminus unterschiedlich Verwendung findet. Im Folgenden wird aus mehreren in der Literatur gebräuchlichen Begriffsverwendungen eine für diesen Artikel sinnvolle Abgrenzung vorgenommen.[4]

---

[2] Die Themengebiete Corporate Governance, Compliance und Risikomanagement interagieren sehr stark miteinander. Aus diesem Grund wird auch von der Trias „Governance, Risk and Compliance" gesprochen, die eine integrierte Strategie und ein gemeinsames Management erfordert (Klotz und Dorn 2008, S. 7).

[3] Das Vier-Augen-Prinzip besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen werden dürfen. Zielsetzung ist die Fehler-, bzw. Missbrauchsreduktion sowie die Erhöhung der Entscheidungsqualität (Herzog und Stephan 2008, S. 39).

[4] Siehe hierzu u.a. (Amberg und Wiener 2006, S. 3; Bravard und Morgan 2009, S. 25).

> IT-Outsourcing bezeichnet 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.

Die vorliegende Definition beinhaltet, der Zielsetzung dieses Artikels folgend, die vorherige Eigenerstellung, auch wenn das gerade im IT-Segment nicht immer der Fall sein muss. Teilweise werden neuerliche Dienste vom Outsourcing-Partner (zusätzlich) erbracht, die zu keinem Zeitpunkt Bestandteil des auslagernden Unternehmens waren. Fremdbezug wäre stattdessen ein angemessener Begriff. Diese Definition des IT-Outscourcing impliziert zwei wesentliche Stakeholdergruppen, die an einem IT-Outsourcing-Projekt beteiligt sind: das auslagernde Unternehmen und den, beziehungsweise die IT-Dienstleister.

3 Berücksichtigung von Compliance im IT-Outsourcing

Für eine kritische Würdigung von Compliance im IT-Outsourcing wurden empirische Untersuchungen durchgeführt, anhand derer die relevanten Compliance-Anforderungen im IT-Outsourcing identifiziert werden konnten. Die konzeptionellen, theoretischen und empirischen Ergebnisse werden in einem Bezugsrahmen zusammengeführt. Dieser umfasst Zielgrößen, Bedingungen und Aktionsparameter zur Beachtung von Compliance im IT-Outsourcing.

3.1 Empirische Untersuchungen

Ziel der *quantitativen Erhebung* war es, anhand der Befragung möglichst vieler Experten aus den Fachgebieten IT-Outsourcing und/ oder Compliance ein aussagekräftiges Meinungsbild aus der Praxis über die Zusammenhänge von IT-Outsourcing und Compliance zu erhalten. Das Vorgehen der Befragung erfolgte so standardisiert wie möglich und so offen wie nötig. Der Fragebogen setzt sich aus vier Frageblöcken zusammen, die sowohl Hybridfragen als auch Rating-Skalen beinhalteten. Es nahmen 233 Personen an der Befragung teil, wovon 123 den Fragebogen beendeten (53 Prozent). Die Probanden wurden mit Hilfe virtueller sozialer Netzwerke, Internetrecherchen und persönlicher Kontakte identifiziert und rekrutiert. Die Güte der Untersuchung wurde anhand des eingesetzten Fragenkata-

logs, der Triangulation[5] und der Regelgeleitetheit in Form von Standardisierung und Strukturierung von Aufzeichnungen und Auswertungen sichergestellt.[6]

Die *qualitative Erhebung* erfolgte anhand von problemzentrierten Experteninterviews in einer strukturierten Interviewsituation. Mit einem Fragebogen wurde partiell Einfluss auf die Interviewten genommen. Dieser weiche Interaktionsstil war wichtig, da die Thematik ein großes Vertrauensverhältnis zwischen den Interviewpartnern voraussetzt. Die Identifikation der Interviewpartner erfolgte durch die „Auswahl typischer Fälle" (Schnell et al. 2005, S. 12). Neben auslagernden Unternehmen wurden auch IT-Dienstleister und Wirtschaftsprüfer befragt. Grundlage für die Wahl der Interviewpartner, Verantwortungsträger in den Bereichen Compliance und IT-Outsourcing, waren Unternehmen aus möglichst unterschiedlichen Branchen mit verschiedenartig fortgeschrittenen Compliance-Bemühungen. Insgesamt nahmen zehn Experten aus neun Unternehmen an den Interviews teil.

3.2 Bezugsrahmen zur Berücksichtigung von Compliance im IT-Outsourcing

Einem theoretischen Bezugsrahmen liegt nach Kirsch ein schlecht strukturierter Kontext zugrunde: „Ein Bezugsrahmen dient in erster Linie dazu, das Denken über komplexe reale Phänomene zu ordnen und exploratorische Beobachtungen zu leiten (…)" (Kirsch 1981, S. 194). Daher enthält ein Bezugsrahmen sehr allgemein gefasste Aussagen des vagen Vorverständnisses.

Der hier angewendete und in Abbildung 1 dargestellte Bezugsrahmen umfasst Zielgrößen zur Beachtung von Compliance im IT-Outsourcing sowie entsprechende Integrationsbedingungen und Aktionsparameter. Ihr Zusammenspiel trägt zur Klärung der Problematik Compliance im IT-Outsourcing bei. Die Ziele, d.h. (1) die Ermittlung der Auswirkungen von Compliance auf das IT-Outsourcing und (2) die Berücksichtigung der Compliance-Anforderungen im IT-Outsourcing werden als mittelbar disponibel angesehen. Auf sie ist das Gestaltungshandeln ausgerichtet. Es erfolgt die Feststellung von nicht disponiblen Bedingungen. Sie schränken die Gestaltungsmöglichkeiten des IT-Outsourcing ein. Als unmittelbar disponible Größen werden hierauf aufbauend Aktionsparameter sowie Mechanismen zur Berücksichtung von Compliance im IT-Outsourcing entwickelt. Diese wirken unmittelbar auf die Zielerreichung.

[5] Die Triangulation beschreibt jegliche Form von Mehrfachperspektiven, die im Forschungsprozess eingesetzt werden können, so z.B. der Einsatz verschiedener Daten, Theorien, Forscher und Beobachter. Mit ihrer Hilfe sollen Verzerrungen vermindert werden (Schnell et al. 2005, S. 262).

[6] Die vollständige Studie kann bei (Amberg et al. 2009) online abgerufen werden.

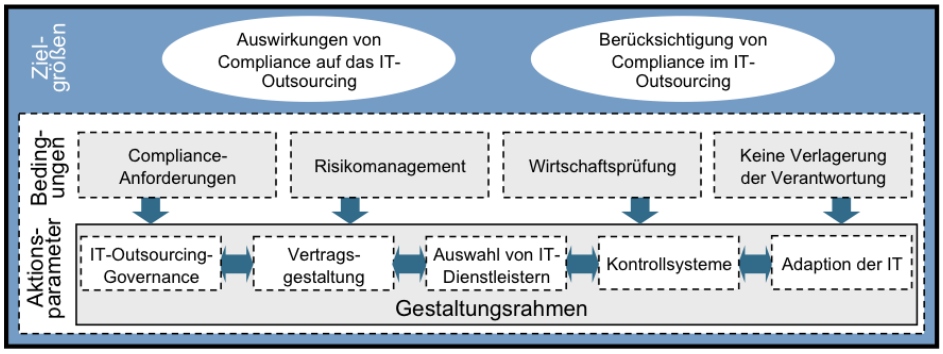

Abbildung 1: Bezugsrahmen zur Ermittlung der Auswirkungen von Compliance und Berücksichtigung von Compliance im IT-Outsourcing

Auswirkungen von Compliance auf das IT-Outsourcing

Die Bedingungen des Bezugsrahmens setzen an den Erkenntnissen der theoretischen Untersuchungen und der empirischen Erhebungen an. Es erfolgt eine Konzentration auf die nachfolgenden Bereiche:

1. Compliance-Anforderungen im IT-Outsourcing
2. Risikomanagement im IT-Outsourcing
3. Wirtschaftsprüfung und IT-Outsourcing
4. Keine Verlagerung der Verantwortung.

Die ermittelten Compliance-Anforderungen (1) sind ausschlaggebend für die Vorgaben, die in einem IT-Outsourcing Beachtung finden müssen. Das Risikomanagement (2) erhält durch Compliance einen besonderen Stellenwert und muss demnach auch im IT-Outsourcing unter der Beachtung von Compliance verstärkt Berücksichtigung finden. Die empirischen Erhebungen haben gezeigt, dass die Zusammenarbeit mit den Wirtschaftsprüfern (3) bei einem IT-Outsourcing an Bedeutung gewinnt. Letztlich wurde die Problematik der Verlagerung der Verantwortung (4) als eine weitere, wichtige Bedingung identifiziert.

(1) Es wurden *Compliance-Anforderungen* im IT-Outsourcing empirisch (quantitativ und qualitativ) evaluiert. Dies erfolgte in Anlehnung an die Ausführungen der BITKOM und einer Erweiterung dieser Ausführungen aufgrund der Sichtung der einschlägigen Literatur (BITKOM 2006). Folglich wurden die Compliance-Anforderungen im IT-Outsourcing sowohl praktisch, theoriebasiert als auch empirisch ermittelt. Die Ergebnisse dieses Zusammenspiels finden sich in Tabelle 1.

Tabelle 1: Analyse von Compliance-Anforderungen im IT-Outsourcing

Compliance-Anforderungen	Ursprung			Relevanz für das IT-Outsourcing		
	D	USA	EU	BITKOM	Qualitative Umfrage	Quantitative Umfrage
KonTraG	X			OO	OOO	OO
GmbHG	X			OO	-	-
HGB	X			OO	-	-
AO	X			O	-	-
BDSG	X			OOO	OOO	OO
SOX		X		OO	OOO	OOO
AktG	X			-	OO	OO
Solvency II				-	-	-
8. EU-Richtlinie			X	-	OO	OO
GDPdU	X			OO	-	-
Basel II			X	O	OO	OO
DCGK	X			-	-	-
GoB/ GoBS	X			OO	-	OO
IDW RS Fait I	X			O	-	O
Interne Richtlinien				-	OOO	OOO

Zu einem einheitlichen Ergebnis kommen die Auswertungen bezüglich des Sarbanes-Oxley Act (SOX.) Er ist das prominenteste Gesetz im Zusammenhang mit Compliance. Diese Aussage hat auch für Compliance-Anforderungen im IT-Outsourcing Geltung. SOX fordert von den betroffenen Outsourcing-Partnern das Vorhandensein eines IKS, welches ein großes Maß an Kontrolle und Governance impliziert (Bravard und Morgan 2009, S. 125). Einfach klingende Vorgaben, wie Aufbewahrungsfristen von Rechnungslegungsdaten oder die vorgeschriebene Kontrolle von Zugangsdaten, erfordern ein Überdenken der vorhanden IT-Sicherheitsmaßnahmen, eine Überarbeitung oder einen Austausch von Applikationen oder Software und nehmen Einfluss auf das IT-Outsourcing.

Das KonTraG wurde übereinstimmend in allen Untersuchungen als wichtiges Gesetz im Zusammenhang mit IT-Outsourcing identifiziert. Die 8. EU-Richtlinie, auch bekannt unter dem Namen „Euro-Sox", hat die BITKOM nicht thematisiert. Dieses widerspricht den Ergebnissen der empirischen Erhebungen.[7]

Basel II wurde in allen Untersuchungen als wichtig interpretiert. Es gilt unmittelbar für Wertpapierfirmen und Kreditinstitute und in keiner Weise für Unternehmen, die keinen Bankkredit in Anspruch nehmen oder in Anspruch zu nehmen

[7] Die 8. EU-Richtlinie wurde durch die Veröffentlichung des BilMoG im Deutschen Bundesanzeiger am 29. Mai 2009 in nationales Recht umgesetzt wurde.

gedenken. Basel II konzentriert sich auf finanztechnische Eigenschaften und nicht auf IT-sicherheitstechnische Angelegenheiten (Klotz 2007b, S. 96-98).[8]

(2) Bereits das Auslagern von einfachen IT-Dienstleistungen birgt das Risiko, dass Zulieferer Standards nicht einhalten oder gegen Gesetze verstoßen. Daher ist die Einrichtung eines *Risikomanagementsystems* unabdingbar geworden. Auch der Gesetzgeber fordert eine solche Maßnahme. „Risiken werden insbesondere in den Gesetzen KonTraG, SOX, BDSG, KWG, Basel II, BaFin (…) angesprochen, die während eines Outsourcing-Projekts ein striktes Risiko-Management erfordern" (BITKOM 2006, S. 17). Durch das KonTrag und Basel II ist das Bewusstsein für die Notwendigkeit eines Risikomanagementsystems auch auf den oberen Führungsebenen vorhanden, jedoch nicht durchgängig, wie Oecking und Kampffmeyer (2007, S. 200)[9] betonen.

Eine Unterscheidung in technische und organisatorische Risiken erscheint für das IT-Outsourcing unter der Berücksichtigung von Compliance sinnvoll (Kampffmeyer 2007, S. 22). Es sollten jedoch auch die operationellen Risiken erwähnt werden, da ein operationelles Risiko nach Basel II mit Eigenkapital zu unterlegen ist.[10]

(3) Das IT-Outsourcing hat in einigen Fällen unmittelbar Auswirkungen auf die Jahresabschlussprüfung. Dies ist bspw. der Fall, wenn Teile der Buchhaltung oder des Rechnungswesens von der Auslagerung betroffen sind. Die Konsequenz ist eine tragende Rolle des Wirtschaftsprüfers des auslagernden Unternehmens. Er muss potentielle Einflüsse auf die Rechnungslegung, bestandsgefährdende Risiken und Beeinträchtigungen der Ordnungsmäßigkeit identifizieren. Hierzu kann der Wirtschaftsprüfer des auslagernden Unternehmens die IT-Organisation, das IKS, die IT-Infrastruktur, die IT-Anwendungen, IT-gestützte Geschäftsprozesse und die IT-Kontrollen des IT-Dienstleisters überprüfen. Ausführungen hierzu finden sich bei Amberg und Mossanen (2008).

(4) Die Vorstellung, dass durch ein IT-Outsourcing auch die *Verantwortung für die ausgelagerten Leistungen* auf den IT-Dienstleister übergeht, ist eine fehlerhafte Annahme. „Werden bestimmte Aufgaben oder Geschäftsprozesse an ein Dienstleistungsunternehmen ausgelagert, so verbleibt die Verantwortung für deren ordnungsmäßige, sichere und gesetzeskonforme Abwicklung bei der Geschäftsführung des Auftraggebers" (Bitkom 2006, S. 18).

---

[8] Eine ausführliche Analyse von Klotz kommt zu dem Schluss, dass das IT-Sicherheitsmanagement nur unwesentlich die Kreditkonditionen beeinflusst (Größenordnung von ca. 1,5 Prozent). Er konstatiert jedoch unternehmensindividuelle Unterschiede. IT-Unternehmen und IT-Dienstleister spricht er explizit an und erwähnt die informations- und kommunikationstechnische Infrastruktur (Klotz 2007b, S. 100).

[9] Bei einer Online-Befragung von „Economist Intelligence" gaben 54 Prozent der 195 befragten Führungskräfte an, dass kein Ausschuss vorhanden ist, der sich aktiv mit Fragen bezüglich Corporate Governance, Risikoprävention oder Compliance auseinandersetzt. Das Vorgehen erfolgt vor allem reaktiv (Oracle 2008).

[10] Operationelles Risiko: „Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen infolge externer Ereignisse eintreten" (Baseler Ausschuss 2004, in: Klotz 2007b, S. 96).

Aktionsparameter für die Berücksichtigung von Compliance im IT-Outsourcing

Unter Einbeziehung der Bedingungen des Bezugsrahmens wird in diesem Abschnitt spezifiziert, welche Möglichkeiten zur Verfügung stehen, angemessen auf die Auswirkungen von Compliance im IT-Outsourcing zu reagieren. Bezug nehmend auf die empirischen Erhebungen und der Sichtung der einschlägigen Literatur können fünf Aktionsparameter für die Berücksichtigung von Compliance im IT-Outsourcing abgeleitet werden:

1. IT-Outsourcing-Governance
2. Integration von Compliance in den IT-Outsourcing-Vertrag
3. Auswahl von IT-Dienstleistern
4. Kontrollsysteme
5. Adaption der Informationstechnologie.

Im Rahmen der Aktionsparameter wurden Mechanismen entwickelt, welche für die Berücksichtigung von Compliance im IT-Outsourcing genutzt werden können. Abbildung 2 fasst diese in einem Gestaltungsrahmen zusammen.

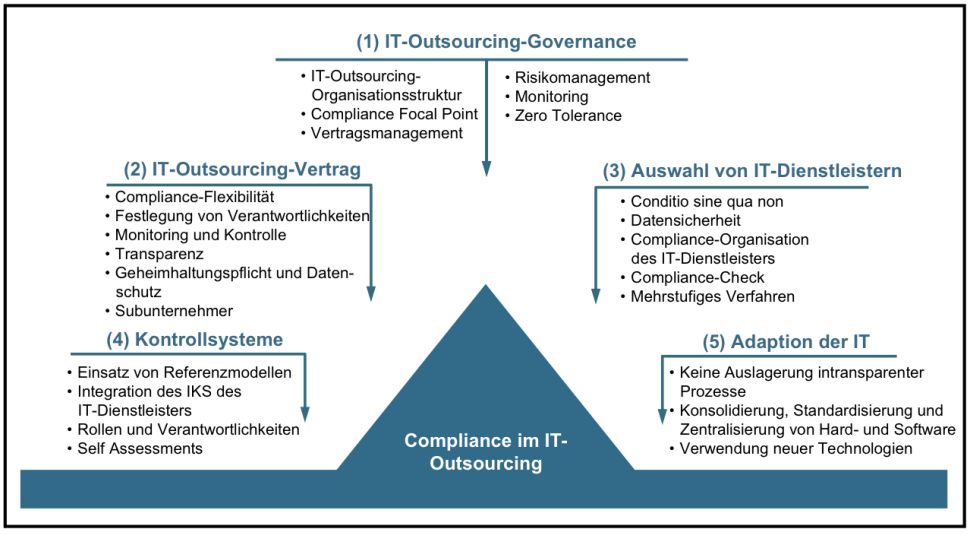

Abbildung 2: Aktionsparameter und Mechanismen zurBerücksichtigung von Compliance im IT-Outsourcing

(1) Unter der *IT-Outsourcing-Governance* wird „(…) die zielgerichtete Gestaltung und Steuerung der Geschäftsbeziehung zum Zwecke der Realisierung gemeinsamer Geschäftsziele von Kunde und Dienstleister verstanden. Dazu muss Governance

sowohl die Kontrolle als auch die Koordination der Geschäftsbeziehung ermöglichen“ (Behrens und Schmitz 2005, S. 28).

Die Organisation des Bezugs von IT-Dienstleistern stellt unter der Beachtung von Compliance eine neue Herausforderung an die IT-Outsourcing-Governance dar. Eine vertrauensbasierte Partnerschaft wird durch Compliance in vielen Bereichen untersagt, da Compliance vermehrt Kontrollen fordert. Dadurch werden Kompatibilitäts- und Kollaborationsprobleme von auslagerndem Unternehmen und IT-Dienstleistern zusätzlich verstärkt. Dieses kann sich in den Organisationsformen, unterschiedlichen Unternehmenskulturen oder in der IT-Infrastruktur bemerkbar machen. Compliance bewegt sich gerade im IT-Outsourcing zwischen der Konformität und dem unternehmerischen Erfolg, die es durch gezielte Maßnahmen zu vereinen gilt (Hofmann und Höberl 2008, S. 8).

Eine solche Maßnahme kann eine Optimierung der IT-Outsourcing-Organisationsstruktur anhand von klar definierten Schnittstellen und Berichtslinien darstellen. Es bietet sich an, einen Compliance Focal Point (definierter Compliance-Ansprechpartner) zu implementieren und ein Vertragsmanagementteam zur kontinuierlichen und proaktiven Vertragsanpassung aufzusetzen. Durch ein „Risk Management Board“ können Compliance-Anforderungen und –Risiken frühstmöglich erkannt und berücksichtigt werden. Monitoring- und Kontrollgreminen ermöglichen standardisierte Audits, Reportings und Analysen, wobei Zero Tolerance bei Non-Compliance gelebt werden sollte.

(2) Es ist eine nachvollziehbare Forderung der auslagernden Unternehmen, dass die wirtschaftlichen und die technischen Vorgaben sowie die Compliance-Anforderungen juristisch in einem *IT-Outsourcing-Vertrag* festgehalten werden. Um den Compliance-Anforderungen gerecht zu werden, bedarf es vertraglicher Bestimmungen, die zum einen die Verantwortung für die Einhaltung rechtlicher Rahmenbedingungen, zum anderen aber auch die Steuerungs- und Kontrollrechte des auslagernden Unternehmens regeln.

Aus Compliance-Sicht sollte ein IT-Outsourcing-Vertrag „Compliance-Flexibilität“ in Form von Anpassungsmöglichkeiten an sich verändernde, gesetzliche Rahmenbedingungen unter Beachtung der potentiellen Mehrkosten beinhalten. Dokumentationspflichten und Verantwortlichkeiten müssen klar definiert werden, z.B. durch Erstellung einer Zuständigkeitenmatrix mit Mitwirkungspflichten der Vertragspartner. Transparenz von Prozessen kann anhand von graphischen Darstellungen und bisweilen durch Einblick in die Systeme der IT-Dienstleister generiert werden. Die Beauftragung von Subunternehmern sollte bei Notwendigkeit von vornherein ausgeschlossen oder ein Mitspracherecht, bzw. ein Vetorecht, bei der Auswahl potentieller Subunternehmer vereinbart werden. Im Rahmen von Monitoring und Kontrolle sollten Messgrößen, Messzeiträume und Häufigkeit der Messungen definiert werden. Hier findet zumeist eine Verwendung des SAS 70 statt, wobei manuelle Kontrollen soweit wie möglich auszuschließen sind.

(3) Die empirischen Erhebungen haben gezeigt, dass bei der *Auswahl von IT-Dienstleistern* zunehmend das Kriterium Compliance einen wichtigen Auswahlfaktor

darstellt. Somit ist Compliance eine Conditio sine qua non – eine grundlegende Anforderung, welche die überwiegende Mehrheit der auslagernden Unternehmen an die IT-Dienstleister stellt. Auslagernde Unternehmen sollten prüfen, ob der IT-Dienstleister tatsächlich in der Lage ist, die individuellen Compliance-Anforderungen zu erfüllen. Referenzen, wie SAS 70-Reporte oder ISO-Zertifizierungen, senden entsprechende Signale. Bei den IT-Dienstleistern ist sowohl auf die physische Datensicherheit (Sicherheit von Daten und Applikationen sowie Backup und Wiederherstellung), als auch auf die logische Datensicherheit zu achten.

Es empfiehlt sich im Rahmen der Due Dilligence zu verifizieren, ob der IT-Dienstleister eine dedizierte Compliance-Organisation implementiert hat. Hierzu gehören, neben weiteren Aspekten, Ansprechpartner, zertifizierte Sicherheitsexperten, Trainingsmaßnahmen und ein ausreichendes Budget für Compliance. Ein Compliance-Check überprüft, ob der IT-Dienstleister oder eines seiner Subunternehmen schon einmal in einen Compliance-Vorfall verwickelt war. Cao et al. schlagen ein zweistufiges Vorgehen bei der Auswahl eines IT-Dienstleisters vor (Cao und Leggio 2008, S. 182). In einem ersten Schritt sollen sich potentielle Partner in Pilotprojekten engagieren, bzw. beweisen. In einem zweiten Schritt werden Verträge nur jenen IT-Dienstleistern angeboten, die sich zuvor bewährt haben.

(4) Die Verwendung von *Kontrollsystemen* und *Referenzmodellen* wie COSO, COBIT oder auch ITIL stellt ein etabliertes Vorgehen im IT-Outsourcing dar. COSO und COBIT sind von den Wirtschaftsprüfern verwendete Prüfmodelle. Aus Gesetzen wie SOX, Basel II oder dem BilMoG leitet sich sowohl direkt, als auch indirekt die Pflicht des Vorhandenseins eines leistungsfähigen IKS, gestützt auf Referenzmodelle, bei den Outsourcing-Partnern ab. Die Implementierung eines IKS in einer IT-Outsourcing-Beziehung birgt neben dem Implementierungsaufwand und der Kosten auch eine Reihe von Vorteilen: Prozesse werden optimiert und transparent, Service- und Reportingkosten reduziert, Bedrohungen frühzeitig erkannt, Redundanzen verringert, der Automatisierungsgrad erhöht, der Mitarbeitereinsatz für Compliance verringert und die Risikobewertung verbessert (Brauer et al. 2009, S. 5, 59).

Es empfiehlt sich die Benennung von „Process-Ownern“, die zur Identifikation, Analyse und Dokumentation der Risiken und Prozesse in Kooperation mit dem „Control-Ownern“ verantwortlich sind. Die „Control-Owner“ sind zuständig für die Umsetzung der interaktiven Kontrolle in ihrem Geschäftsprozess.

(5) Wie eingangs erwähnt, kommt der IT eine Schlüsselrolle beim Erreichen von Compliance zu, weshalb die *Adaption der IT* von Bedeutung ist.

Die Wahl der richtigen Software ist ein kritischer Faktor beim Erreichen von Compliance. Daher bietet IT-Outsourcing die Möglichkeit, Systemlandschaften zu bereinigen und IT-Prozesse zu standardisieren. Es kann von historisch gewachsenen Systemen und Applikationen, bei denen bspw. Dokumentationen nicht ausreichend vorhanden sind oder kein Berechtigungsmanagement existiert, auf „State-of-the-Art“-Lösungen migriert werden. Hierdurch werden risikobehaftete Integrati-

onslösungen zwischen Individualsoftware und Standardsoftware reduziert. Ein IT-Outsourcing ermöglicht zumeist auch eine stärkere Zentralisierung, die gerade für die IT-Compliance von den Experten gefordert wird. IT-Systeme nur für Compliance einzuführen ist unwirtschaftlich. Es gilt also, das Nutzenpotential der IT auf dem Weg zu Compliance auszuschöpfen. Neue IT-Lösungen sollten anerkannte und getestete Technologien zur Automatisierung von Kontrollen, zur Verbesserung der Compliance-Effizienz und zur Erhöhung der Profitabilität sein.

4 Fazit und Ausblick

Durch die literaturbasierten Recherchen und die empirischen Erhebungen konnten für das IT-Outsourcing relevante Compliance-Anforderungen und entsprechende Gestaltungsempfehlungen identifiziert, bestätigt und besser eingeordnet werden. Diese Erkenntnisse sind Teil der Untersuchungen des Bezugsrahmens und lassen einen zusätzlichen Handlungsbedarf bei der Durchführung von IT-Outsourcing erkennen.

Alle Studienteilnehmer waren sich einig darüber, dass Compliance zukünftig an Relevanz im IT-Outsourcing zunehmen wird. Die Fragestellung, welche Vertragspartei mehr Compliance-Know-how in eine IT-Outsourcing-Beziehung einbringt, konnte nicht ohne Weiteres beantwortet werden. Grundsätzlich haben die IT-Dienstleister das operative Know-how und zumeist die größere Expertise. Allerdings zeigt sich in einigen Branchen, bspw. in der Finanzbranche, dass die Outsourcing-Kunden größere Compliance-Erfahrungen besitzen.

Diese Erkenntnisse erfordern auch zukünftig eine intensive Auseinandersetzung in Wissenschaft und Praxis mit der Berücksichtigung von Compliance im IT-Outsourcing, der Ermittlung der diskriminierenden Compliance-Faktoren, der Entwicklung von Gestaltungsempfehlungen sowie deren praktische Umsetzung.

Literatur

Amberg M, Mossanen K, Biermann, S (2009) Compliance im IT-Outsourcing – Theoretische und empirische Ermittlung von Einfluss nehmenden Compliance-Faktoren. http://www.wi3.uni-erlangen.de/index.php?id=78.

Amberg M, Mossanen K (2008) Compliance im IT-Outsourcing. In: Hildebrand K, Meinhardt M (Hrsg.) Compliance & Risk Management. HMD 263. dpunkt, Heidelberg, S. 58-68.

Amberg M, Wiener M (2006) IT-Offshoring – Management internationaler IT-Outsourcing-Projekte. Physica, Heidelberg.

Behrens S, Schmitz C (2005) Ein Bezugsrahmen für die Implementierung von IT-Outsourcing-Governance. In: Strahringer S (Hrsg.) Outsourcing, HMD 245. dpunkt, Heidelberg, S. 28-36.

BITKOM (2006) Compliance in IT-Outsourcing-Projekten – Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen. Berlin

Böhm M (2008): IT-Compliance als Triebwerk von Leistungssteigerung und Wertbeitrag der IT. In: Hildebrand K, Meinhardt S (Hrsg.) Compliance & Risk Management, HMD 263. dpunkt, Heidelberg, S. 15-29.

Bräutigam P, Hartwig G (2004) Rechtliche Ausgangspunkte. In: Bräutigam P (Hrsg.) IT-Outsourcing. Schmidt, Berlin, S. 162-203.

Brauer MH, Steffen KD, Biermann S, Schuler AH (2009) Compliance Intelligence. Schäffer-Poeschel, Stuttgart.

Bravard JL, Morgan R (2009) Intelligentes und erfolgreiches Outsourcing. FinanzBuch, München.

Cao Q, Leggio K (2008) Applying the Real Option Approach to Vendor Selection in IT-Outsourcing. In: Olson D, Wu D (Hrsg.) New Frontiers in Enterprise Risk Management. Springer, Heidelberg, S. 181-192.

Gadatsch A (2006) IT-Offshore realisieren. Vieweg, Wiesbaden.

Hauschka C (2008): Einführung. In: Umnuß K (Hrsg.) Corporate Compliance Checklisten. Beck, München.

Hofmann T, Höberl P (2008) Krisen- und Risikomanagement. In: Management Circle Verlag GmbH, Compliance Management, Lektion 8, Eschborn.

Kampffmeyer U (2007) Information Management Compliance. http://www.project-consult.net/Files/Compliance%5FKampffmeyer%5F20070926.pdf.

Kirsch W (1981) Über den Sinn der empirischen Forschung. In: Witte E (Hrsg.) Der praktische Nutzen empirischer Forschung. Siebeck, Tübingen, S. 189-229.

Kley KL (2008) Controlling im Spannungsfeld von Governance und Vertrauen. In: Horváth P (Hrsg.) Mehr Verantwortung für den Controller. Schäffer-Poeschel, Stuttgart, S. 3-16.

Klotz M, Dorn DW (2008) Begriff, Umfang und relevante Regelwerke. In: Hildebrand K, Meinhardt S (Hrsg.) Compliance & Risk Management. HMD 263, dpunkt, Heidelberg, S. 5-14.

Klotz M (2007a) IT-Compliance. In: IT-Governance, ISACAGermany (1), S. 14-18.

Klotz M (2007b) Basel II als Treiber des IT-Sicherheitsmanagements. In: Fröschle, HP, Strahringer S (Hrsg.) IT-Industrialisierung, HMD 256, dpunkt, Heidelberg, S. 93-104.

Oecking C, Kampffmeyer H (2007) Operatives IT-Risikomanagement. In: Gründer T, Schrey J (Hrsg.) Managementhandbuch IT-Sicherheit. Schmidt, Berlin, S. 181-201.

Oracle (2008) Einhaltung von ComplianceRichtlinien. http://www.compliance magazin.de/plaintext/markt/studien/oracle110908.html.

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

Schnell R, Hill PB, Esser E (2005) Methoden der empirischen Sozialforschung, Oldenbourg, München.