

Compliance im IT-Outsourcing

Theoretische und empirische Ermittlung von
Einfluss nehmenden Compliance-Faktoren

Eine gemeinschaftliche Studie der
Friedrich-Alexander-Universität Erlangen-Nürnberg
Lehrstuhl für Wirtschaftsinformatik III
und
Accenture


High performance. Delivered.







I. Ausschlussklausel

Inhalt der Studie

Die in dieser Studie bereitgestellten Informationen entsprechen unserem Kenntnisstand zum Veröffentlichungszeitpunkt. Sie können sich verändern, sofern neue Erkenntnisse vorliegen.

Die Friedrich-Alexander-Universität Erlangen-Nürnberg und Accenture übernehmen keinerlei Gewähr für die Aktualität, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen die Friedrich-Alexander-Universität Erlangen-Nürnberg oder Accenture, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

Die Autoren behalten es sich ausdrücklich vor, Teile der Seiten oder die gesamte Studie ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Urheber-, Marken-, Patent- und andere Schutzrechte

Sämtliche Inhalte der Studie einschließlich der Texte und grafischen Darstellungen sind das geistige Eigentum der Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Wirtschaftsinformatik III, oder von Accenture bzw. Dritten und dürfen ohne vorherige schriftliche Zustimmung nicht für öffentliche oder gewerbliche Zwecke vervielfältigt, verändert, übertragen, wieder verwendet, neu bereitgestellt, verwertet oder auf sonstige Weise genutzt werden.

Alle in der Studie genannten und gegebenenfalls durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweilig eingetragenen Eigentümer.

II. Gliederung der Studie

I.	Ausschlussklausel	1
II.	Gliederung der Studie	2
III.	Vorwort	3
IV.	Management Summary	5
V.	Abkürzungsverzeichnis	7
VI.	Abbildungsverzeichnis	9
1.	Einführung: IT-Outsourcing & Compliance.....	10
2.	Zielsetzung und Aufbau der Studie	12
3.	Einordnung und Abgrenzung von Compliance und IT-Outsourcing	13
3.1.	Compliance	13
3.2.	IT-Outsourcing	18
3.2.1.	Definition und Entwicklung	18
3.2.2.	Formen des IT-Outsourcing.....	20
3.2.3.	Argumentenbilanz des IT-Outsourcing	24
4.	Rechtliche Rahmenbedingungen von Compliance und IT-Outsourcing	30
4.1.	Gesetzliche Regelungen	31
4.2.	Richtlinien, Standards und Referenzmodelle	34
5.	IT-Outsourcing unter Compliance-Aspekten	46
5.1.	Pro IT-Outsourcing	46
5.2.	Contra IT-Outsourcing	48
6.	Empirische Untersuchung	51
6.1.	Relevante Gesetze für das IT-Outsourcing	52
6.2.	Rahmenwerke, Zertifikate und Standards beim IT-Outsourcing	53
6.3.	Compliance als Argument pro oder contra IT-Outsourcing	54
6.3.1.	Allgemeine Bedeutung von Compliance für IT-Outsourcing-Entscheidungen	54
6.3.2.	Einfluss von Compliance Anforderungen bei konkreten IT-Outsourcing-Entscheidungen.....	55
7.	Compliance in der Outsourcing-Praxis.....	58
7.1.	Accenture – das Unternehmen.....	58
7.2.	Die zunehmende Bedeutung von Compliance für Outsourcing am Beispiel von British Telecom (BT).....	60
7.3.	Praxisorientierte Maßnahmen zur Beachtung von Compliance für Outsourcing	63
8.	Fazit.....	71
VII.	Literaturverzeichnis	74
VIII.	Autoreninformationen	77
IX.	Accenture	79

III. Vorwort



Compliance Management ist eine Thematik, die zunehmend auch einen Forschungsgegenstand an deutschen Hochschulen darstellt. Dieses hoch aktuelle, aber dennoch äußerst komplexe und schwer erfassbare Thema verbindet unterschiedliche Disziplinen miteinander. Neben der Betriebswirtschaftslehre, Informatik und Rechtswissenschaft setzen sich auch ethische und sozialwirtschaftliche Forschungsbereiche mit dem Thema Compliance auseinander.

Die Anzahl diesbezüglicher Kooperationen zwischen Wissenschaft und Praxis nimmt kontinuierlich zu und stellt einen wichtigen Bestandteil in der Erforschung dieses Themengebiets dar. Deshalb ist die vorliegende Studie ein wichtiger Schritt zur Untersuchung des IT-Outsourcing im Zusammenhang mit Compliance und der Reduktion von Ungewissheiten. Sie greift insbesondere die Fragestellung auf, ob Compliance ein zu berücksichtigendes Kriterium im IT-Outsourcing darstellt, leistet eine tiefgehende Analyse der Problematik und zeigt Antworten auf. Durch die Kooperation zwischen Wissenschaft und Praxis konnten somit Synergien geschaffen und besonders wertvolle Erkenntnisse erzielt werden.

Der Lehrstuhl für Wirtschaftsinformatik III, insbesondere Betriebswirtschaftslehre, der Friedrich-Alexander-Universität Erlangen-Nürnberg hat als einer der ersten Lehrstühle in Deutschland das Thema Compliance, insbesondere IT-Compliance, im Rahmen der Wirtschaftsinformatik aufgegriffen und zu seinem Forschungsgegenstand erklärt. Innerhalb der Forschungsaktivitäten und Kooperationen mit Praxispartnern konnten interessante Erkenntnisse erzielt und publiziert werden.

Wir freuen uns, Ihnen zusammen mit der weltweit agierenden Unternehmensberatung Accenture die aktuellen Entwicklungen und einen Ausblick zum Thema Compliance im IT-Outsourcing präsentieren zu können und hoffen, dass die Ergebnisse dieser Studie wertvolle Hinweise liefern, die Sie für sich nutzen können.

Prof. Dr. Michael Amberg
Dipl.-Kfm. Kian Mossanen
Dipl.-Vw. Winfried Kramolisch

FAU Erlangen-Nürnberg

Dipl.-Bw. Sven Biermann (MBA)
Dr. Leo Lehr

Accenture

Lehrstuhl für Wirtschaftsinformatik III, insbesondere Betriebswirtschaftslehre
Prof. Dr. Michael Amberg

Kontakt:

amberg@wiso.uni-erlangen.de

kian.mossanen@wiso.uni-erlangen.de

winfried.kramolisch@wiso.uni-erlangen.de

sven.biermann@accenture.com

leo.lehr@accenture.com



IV. Management Summary

Kostendruck, die Standardisierung von bestehenden Prozessen sowie die Fokussierung auf unternehmerische Kerntätigkeiten sind häufig die treibenden Faktoren, warum sich Unternehmen im zunehmenden Wettbewerb einer multipolaren Welt mit Outsourcing beschäftigen. Dies muss jedoch immer auch vor dem Hintergrund ordnungsgemäßen Handelns geschehen, denn eine Verlagerung von Geschäftstätigkeiten bedeutet nicht die Verlagerung der unternehmerischen Verantwortung.

Der Lehrstuhl für Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik, der Friedrich-Alexander-Universität Erlangen-Nürnberg und der weltweit agierende Managementberatungs-, Technologie- und Outsourcing-Dienstleister Accenture haben sich dieser Thematik angenommen und mit der vorliegenden Studie die Zusammenhänge von IT-Outsourcing und Compliance analysiert. Dazu werden einleitend die grundlegenden Annahmen und Definitionen erläutert, die gesetzlichen Regelungen dargestellt und ein Überblick über bewährte Referenzmodelle, Zertifizierungen und Verfahren gegeben. Im Rahmen einer Argumentationsbilanz wird das IT-Outsourcing beleuchtet und mit Pro- und Contra-Argumenten kritisch bewertet.

Darauf aufbauend folgt im praxisorientierten Teil der Studie die Darstellung der Ergebnisse einer quantitativen Erhebung über die Zusammenhänge von IT-Outsourcing und Compliance. Mit der Teilnahme von 132 Experten¹ aus den Bereichen Compliance und/oder Outsourcing liefert sie ein aussagekräftiges Meinungsbild aus der Praxis. Die Rücklaufquote von 56% unterstreicht die Aktualität dieser Thematik.

Abschließend werden die theoretischen Erkenntnisse und die quantitativen Analysen anhand eines konkreten Outsourcing-Projekts bestätigt sowie praktische Maßnahmen zur Beachtung von Compliance dargestellt.

¹ Insgesamt wurden 233 Experten aus allen Industrien befragt.

Die vorliegende Studie bestätigt, dass Compliance ein wichtiger Aspekt im Outsourcing darstellen muss, dieses aber teilweise noch nicht so gesehen wird. Allerdings können auslagernde Unternehmen die Verantwortung für ihre Geschäftstätigkeiten nicht an den Outsourcing-Dienstleister übertragen; die Sicherstellung von Konformität mit gesetzlichen Regelungen, Richtlinien und innerbetrieblichen Bestimmungen muss daher integraler Bestandteil des gesamten Auslagerungsprozesses sein.



V. Abkürzungsverzeichnis

AAA	American Accounting Association
AO	Abgabenordnung
ASP	Application Service Providing
ATCAT	Accenture Transaction Compliance & Analytics Tool
BDSG	Bundesdatenschutzgesetz
BilMoG	Bilanzrechtsmodernisierungsgesetz
BMF	Bundesministerium für Finanzen
BPO	Business Process Outsourcing
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCM	Continuous Controls Monitoring
COBIT	Control Objectives for Information and related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DCF	Discounted Cash Flow
DCGK	Deutscher Corporate Governance Kodex
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FAIT	Fachausschuss für Informationstechnik
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GRC	Governance, Risk und Compliance
GSHB	Grundschutzhandbuch
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer
IKS	Internes Kontrollsystem
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library

KonTraG	Kontroll- und Transparenzgesetz
KWG	Kreditwesengesetz
OPW	Operational Process Workbench
PCAOB	Public Companies Accounting Oversight Board
PS	Prüfungsstandard
RS	Rechnungslegungsstandard
SAS	Statement on Auditing Standards
SCM	Supply Chain Management
SEC	Securities and Exchange Commission
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act
VPN	Virtual Private Networks



VI. Abbildungsverzeichnis

Abbildung 1: Zusammenspiel von Risiken, Governance und Compliance (eigene Darstellung).....	18
Abbildung 2: Klassifizierung von IT-Outsourcing (in Anlehnung an Amberg/Wiener).....	23
Abbildung 3: Argumentenbilanz des IT-Outsourcing (eigene Darstellung).....	29
Abbildung 4: IT-Outsourcing relevante Regelungen (eigene Darstellung).....	52
Abbildung 5: Beurteilung der Aussage „Compliance spielt bei IT- Outsourcing-Entscheidungen eine wichtige Rolle“ (eigene Darstellung).....	54
Abbildung 6: Compliance als Pro- bzw. Contra-Argument beim IT- Outsourcing (eigene Darstellung).....	56
Abbildung 7: Beurteilung der Frage „Erhöhen Compliance Anforderungen die Kosten des IT-Outsourcing?“ (eigene Darstellung).....	57
Abbildung 8: Accenture Delivery Network (eigene Darstellung).....	59
Abbildung 9: Rollen und Verantwortlichkeiten des Contract Manager (eigene Darstellung).....	66
Abbildung 10: Operational Excellence (eigene Darstellung).....	67

1. Einführung: IT-Outsourcing & Compliance

Das IT-Outsourcing, die Auslagerung von IT-Infrastrukturen und Applikationen sowie von Geschäftsprozessen mit hohem IT-Anteil, ist kein neuer strategischer Ansatz. Die Outsourcing-Bewegungen der vergangenen Jahre haben vielmehr alle Teile der Unternehmen erfasst. Durch die Auslagerung von Unternehmens-IT und/oder Prozessen erhoffen sich viele Unternehmen einen kompetitiven Vorteil. Allerdings steht letzteres nicht mehr alleine im Fokus der Entscheidungsfindung für oder gegen Outsourcing. Themen wie Innovation und kontinuierliche Qualitätsverbesserung gewinnen verstärkt an Bedeutung. Laut Dr. Stephan Scholtissek, Vorsitzender der Geschäftsführung von Accenture, wird „klassisches, kostenorientiertes IT-Outsourcing mehr und mehr durch ein wert-, geschäfts- und innovationsorientiertes Outsourcing abgelöst.“

Zudem steigt die Anforderung, sich in einem immer komplexer werdenden, globalisierten Umfeld auf neuen Konsumenten-, Beschaffungs- und Absatzmärkten zu behaupten. Hierfür gilt es, Unternehmen (Organisation, Prozesse und Informationssysteme) flexibel an sich ständig ändernde Rahmenbedingungen anzupassen. Der anhaltende Trend der Internationalisierung bietet neben Chancen etwa durch Ausnutzung von Kostenarbitragen, dem Zugang zu hochqualifizierten Fachkräften oder der Nutzung aufstrebender Innovationszentren auch nicht zu unterschätzende Herausforderungen. Speziell international aufgestellte Unternehmen stehen vor der Herausforderung, eine wachsende Zahl an verschiedenen juristischen, politischen oder gesellschaftlichen Regeln und Rahmenbedingungen einhalten zu müssen (Compliance). Eine Studie der Unternehmensberatung Accenture, bei der über 350 Finanzvorstände in 30 Ländern befragt wurden, ergab zwei Kernkompetenzen als entscheidende Erfolgsfaktoren zur Begegnung globaler Herausforderungen: die Bereitstellung standardisierter Prozesse und die Einhaltung von regulatorischen Vorgaben [Accenture 2008, S. 11].

Compliance gewinnt aufgrund der steigenden Zahl internationaler Vorgaben wie dem Sarbanes-Oxley Act (SOX), Basel II oder der 8. EU-Richtlinie (mit deren Umsetzung in deutsches Recht durch das Bilanzrechtsmodernisierungsgesetz (BilMoG)) zu-



nehmend an Bedeutung. Dabei verstärken die jüngsten Compliance-Untersuchungen sowie Urteile die Sorge, selbst in eine unangenehme Compliance-Situation zu geraten, bzw. in der Öffentlichkeit als nicht verantwortungsbewusst angesehen zu werden.

Auch wenn viele deutsche Unternehmen nicht direkt den teilweise international wirkenden Compliance-Vorgaben (etwa dem Sarbanes-Oxley Act) unterliegen, so interessieren sich global agierende Kunden verstärkt auch für die internen Prozesse ihrer Lieferanten [BITKOM 2006, S. 14]. Es entstehen Problemfelder und Fragen, die in der aktuellen Compliance-Diskussion noch nicht umfassend thematisiert worden sind und denen insbesondere beim IT-Outsourcing Beachtung geschenkt werden sollte. Auslagernde Unternehmen erkennen daher zunehmend die Bedeutung von Compliance sowohl bei der Entscheidungsfindung für oder gegen Outsourcing als auch bei dem nachfolgenden, operativen Betrieb.

2. Zielsetzung und Aufbau der Studie

Aufgrund der Aktualität der Problemstellung verbindet vorliegende Studie die Themen „IT-Outsourcing“ und „Compliance“ zu einer Einheit und unterzieht diese Fusion einer kritischen Betrachtung. Es wird untersucht, warum Compliance beim IT-Outsourcing eine Schlüsselrolle einnimmt, obwohl bis dato Compliance in der Regel als Entscheidungskriterium vernachlässigt wurde. Der Leser erhält einen Überblick über das Zusammenspiel der Themen IT-Outsourcing und Compliance und kann daraus Erkenntnisse für sich und seine Anforderungen ableiten. Neben der theoretischen Analyse der Thematik trägt der praxisorientierte Teil dazu bei, die theoretischen Ausführungen verständlicher darzulegen und dem Leser Praxisbeispiele an die Hand zu geben. Nach dem Lesen dieser Studie soll ein klares Verständnis bezüglich der kritischen Faktoren beim IT-Outsourcing in Verbindung mit Compliance hergestellt werden. Zur Erreichung der Zielsetzung greift die Studie nachfolgende Fragestellungen auf und beantwortet diese:

- Welche Compliance-Anforderungen sind für das IT-Outsourcing relevant?
- Kann die Verantwortung für Compliance durch IT-Outsourcing transferiert werden?
- Welche Compliance-Nachweise und „Best Practices“ setzen sich am Markt durch?
- Stellt Compliance ein Argument für oder gegen das IT-Outsourcing dar?
- Wie können IT-Outsourcing-Projekte compliant realisiert werden?

Zur Erreichung der beschriebenen Ziele und zur Beantwortung der gestellten Fragen gliedert sich die Studie in zwei Teile, den theoretischen und den praktischen Teil.

Im *ersten Teil* werden die Themen Compliance und IT-Outsourcing vorgestellt, die Gesetzeslage analysiert und die Fusion der Themen einer kritischen Würdigung unterzogen.

Im *zweiten Teil* erfolgt eine quantitative Erhebung und Analyse anhand einer Expertenfrage. Zusätzlich werden durch Praxisbeispiele die Bedeutung von Compliance sowie Maßnahmen und Vorgehensweisen zur Beachtung von IT-Compliance im Outsourcing dargestellt.



3. Einordnung und Abgrenzung von Compliance und IT-Outsourcing

3.1. Compliance

Der Begriff **Compliance** stammt aus dem Englischen und bedeutet „Einhaltung“ oder „Befolgung“. Bezogen auf regulatorische Vorgaben, etwa gesetzliche Regelungen, Richtlinien, Standards und Referenzmodelle sowie innerbetriebliche Bestimmungen, ist damit ein konformes Verhalten gemeint. Im Unternehmen stellt Compliance eine Managementaufgabe dar, deren Zweck die Einhaltung aller branchenübergreifenden oder branchenspezifischen Gesetze und Vorschriften ist [Annuschein 2006].

Compliance unterstützt die Transparenz und Kontrolle innerhalb eines Unternehmens, reduziert Risiken und verbessert die Beständigkeit des Geschäftsmodells. Zusätzlich trägt Compliance zu einem verbesserten Ansehen in der Öffentlichkeit und Vertrauen bei Stakeholdern bei [Amberg et al. 2007, S. 13]. Weiter gefasst ist jeder Stakeholder (Mitarbeiter, Lieferanten etc.) in irgendeiner Form Compliance verpflichtet bzw. muss sich compliant verhalten. Bei einer umfassenden Anwendung von Compliance wären global mehr als 10.000 Compliance-Vorschriften zu befolgen.

Compliance obliegt der Verantwortung der Unternehmensleitung und bedarf somit eines unternehmensweiten, bewussten und systematischen Managements. Dieses setzt sowohl die Kenntnis relevanter Regularien und Normen sowie die daraus resultierenden Risiken, als auch das Zusammenspiel aller beteiligten internen und externen Parteien voraus. Compliance ist somit keine Aufgabe, welche ein Geschäftsbereich im Alleingang übernehmen kann oder sollte, sondern eine unternehmensweite Anstrengung über Abteilungsgrenzen hinweg, die wiederum aus dynamischen und kontinuierlichen Prozessen besteht.

Compliance ist ein wesentlicher Bestandteil einer verantwortungsvollen Unternehmensführung. Allerdings sehen sich immer mehr Unternehmen, trotz weit reichender regulatorischer Vorgaben, veranlasst den Aufbau von unternehmensweiten Grundsätzen im Rahmen einer so genannten Corporate Governance vorzunehmen. Corporate Governance beschreibt Werte und Normen innerhalb eines Unterneh-

mens, d.h. die institutionellen und politischen Rahmenbedingungen von Unternehmen, und stellt somit eine Art Unternehmensverfassung dar. Dies ist vor allem aus zwei Gründen sinnvoll: Erstens werden Regularien häufig reaktiv erlassen (ex post). Zweitens können Regularien nicht den Anspruch erheben, jede nur mögliche Situation abzudecken; gerade bei der Auslegung von Unklarheiten bieten Governance-Programme eine Orientierung, um dem Grundsatz der verantwortungsvollen Unternehmensführung gerecht zu werden.

Die Bedeutung von Compliance und Corporate Governance wurde durch die jüngste Erweiterung des Deutschen Corporate Governance Kodex (DCGK) Mitte 2008 noch einmal hervorgehoben, in dem Compliance an verschiedenen Stellen aufgenommen wurde.² Die Verantwortung der Unternehmensleitung (Vorstand oder Geschäftsführung) wird im Rahmen von Compliance ausdrücklich dargestellt [DCGK 2008, Ziffer 4.1.3]:

„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).“

Um dieser Sorgfaltspflicht nachzukommen, muss ein entsprechendes Bewusstsein beim Umgang mit Compliance-relevanten Regularien auch im Zusammenspiel mit internen Kontrollmechanismen gesehen werden. Im Rahmen eines internen Kontrollsystems (IKS) werden dabei Regelungen zur Steuerung der Unternehmensaktivität und Überwachungsmaßnahmen zur Einhaltung dieser Regelungen aufgestellt. Das Institut der Wirtschaftsprüfer (IDW) definiert ein IKS wie folgt [IDW 2006, PS 261.19]:

² Aufgrund der zunehmenden Bedeutung von Corporate Governance setzte das Bundesministerium der Justiz 2001 eine Regierungskommission ein, die 2002 den Deutschen Corporate Governance Kodex (DCGK) verabschiedete und diesen auch weiterhin regelmäßig hinsichtlich Anpassungsbedarfs überprüft. Der DCGK gibt Empfehlungen zur Corporate Governance, also zur Führung und Überwachung von Organisationen. Ziel ist es, das Vertrauen in deutsche Unternehmen zu stärken. Die Empfehlungen werden vom Bundesjustizministerium im amtlichen Teil des elektronischen Bundesanzeigers veröffentlicht. Der 2002 eingefügte § 161 AktG sieht eine Entsprechenserklärung der börsennotierten Unternehmen zum DCGK vor.



„Unter einem internen Kontrollsystem werden die von dem Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements

- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),
- zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
- zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften.“

Ein IKS beinhaltet in seiner Überwachungsfunktion sowohl prozessintegrierte (organisatorische Sicherungsmaßnahmen und Kontrollen) als auch prozessunabhängige Maßnahmen (etwa die Etablierung einer Internen Revision). Dabei muss ein IKS sämtliche Aspekte in Betracht ziehen, die einen Einfluss auf die Geschäftsaktivität, die interne und externe Rechnungslegung sowie die Einhaltung rechtlicher Vorschriften haben. Zur Umsetzung von IKS wird in der Praxis oft auf das COSO-Referenzmodell (vgl. Abschnitt 0) verwiesen.

Die Informationstechnologie nimmt bei der Einhaltung von Compliance eine Schlüsselfunktion ein, was sowohl bei der Auslagerung der IT-Infrastruktur als auch der Auslagerung von ganzen Geschäftsprozessen berücksichtigt werden muss. Zum einen können immer komplexer werdende Geschäftsprozesse und deren zunehmende weltweite Verteilung ohne die Nutzung von Informationstechnologie nicht mehr bewältigt werden. Die Unternehmens-IT, also die IT-Infrastruktur (Netzwerke und Hardware) und die IT-Systeme (transaktionale und unterstützende Applikationen), bildet dafür die Basis, auf der sowohl kaufmännische Prozessschritte als auch andere Aktivitäten durchgeführt werden. Insbesondere transaktionale Applikationen bedürfen eines hohen Augenmerks, da sich Mängel oder gar die Funktionsunfähigkeit dieser Systeme unternehmensweit auswirken und finanzielle Konsequenzen nach sich ziehen können. Zum anderen bieten sich durch die IT selbst auch Möglichkeiten zur

Überwachung der Einhaltung von Compliance im Rahmen eines IKS, bspw. durch automatisierte Kontrollen.

Analog zur unternehmensweiten Corporate Governance muss sich die IT natürlich auch an stringenten Werten und Richtlinien orientieren. Mit **IT-Governance** wird

- die Unterstützung des Unternehmens bei der Erreichung von Geschäftszielen,
- die Ausrichtung der IT an den Unternehmenszielen und -prozessen (IT-Strategie),
- den verantwortungsvollen und nachhaltigen Einsatz von IT-Ressourcen (IT-Mitarbeiter, IT-Systeme und IT-Komponenten) zur Erhöhung der IT-Performance (Regeln und Richtlinien für die IT),
- die Erhöhung der Zufriedenheit von Kunden sowie
- eine Minimierung der IT-Risiken (Ausfallrisiko kritischer Applikationen)

bezeichnet. Die IT-Governance übernimmt die konzeptionelle Planung und Entwicklung von Prozessen als auch IT-relevante interne Kontrollmechanismen. Mit IT-Governance wird somit ein Rahmenwerk vorgegeben, um Compliance auch im Bereich der Informationstechnologie sicherzustellen.

Die **IT-Compliance** ist, aufgrund der Wichtigkeit von Informationstechnologie für das unternehmerische Handeln, eine notwendige Voraussetzung für das Erreichen von Compliance auf Unternehmensebene. Innerhalb der IT-Compliance bezieht sich die Einhaltung von gesetzlichen Regelungen, Richtlinien, Standards und Referenzmodellen sowie innerbetriebliche Bestimmungen auf den Umgang mit der im Unternehmen vorhandenen IT. Demnach ist IT-Compliance ein Zustand, in dem die IT für das Unternehmen relevanten Gesetze oder in ihrer allgemeinen Gestaltungsordnung von diesen abgeleiteten Rechtsnormen nachweislich einhält oder zu deren Einhaltung beiträgt [Klotz 2007, S. 14-18]. IT-Compliance hat zumeist einen eher operativen Charakter und beschäftigt sich mit IT-Kontrollaktivitäten, IT-Audits und IT-Sicherheitsbewertungen.

Insbesondere die Definition, Implementierung, Durchführung und Dokumentation von **IT-Kontrollen** steht im Fokus der IT-Compliance als Bestandteil eines IKS. Hierbei



handelt es sich um Methoden und Prozesse, die sicherstellen, dass für die IT relevante Gesetze und Managementanweisungen vorgabengemäß eingehalten werden. Hierbei können *generelle IT-Kontrollen* (Organisatorische Kontrollen, Sicherheitskontrollen, Entwicklungskontrollen, etc.) und *applikationsspezifische Kontrollen* (Eingabe-, Verarbeitungs- und Ausgabekontrollen) unterschieden werden. Die generellen Kontrollen bilden dabei den Wirkungsrahmen für die Ausführung von Applikationskontrollen, die auf den einzelnen IT-Systemen angewendet werden. Deshalb muss die IT-Governance gewährleisten, dass die IT-Infrastruktur so ausgestaltet und strukturiert ist, dass diese beiden Kontrollarten kompatibel zueinander sind. Außerdem können die beschriebenen IT-Kontrollen *automatisiert* oder *manuell* sowie *präventiv* oder *detektivisch* durchgeführt werden, je nach Bedarf und Anforderung.

Die IT-Compliance gerät zunehmend in die Betrachtung, da der Gesetzgeber in den letzten Jahren verschärfende Gesetze zur Daten- und Informationsqualität erlassen hat. Dieses liegt unter anderem darin begründet, dass wie zuvor erwähnt die Mehrheit der unternehmerischen Geschäftsprozesse IT-Unterstützung benötigt. IT-Compliance wird somit zur Pflicht und ist keine „Kür“. Deutlich wird dies insbesondere bei Enterprise Resource Planning-Systemen (ERP-Systemen), die einen Großteil der unternehmensinternen und teilweise auch der unternehmensexternen Prozesse abbilden. Hier liefert die IT die notwendigen Informationen zur Erfüllung von Compliance auf Gesamtunternehmensebene und erhält daher eine Schlüsselfunktion.

Es lässt sich konstatieren, dass die Themengebiete (IT-)Governance, Risikomanagement³ und (IT-)Compliance sehr stark miteinander interagieren. Die Schnittstellen werden sowohl in der Literatur als auch in der Praxis differenziert dargestellt. Zunehmend findet aber der GRC-Ansatz (Governance, Risk und Compliance) Akzeptanz, der die Themen vereint und in Abbildung 1 dargestellt ist.

³ Risikomanagement: Systematische Erfassung und Bewertung von Risiken und die Steuerung von Reaktionen auf festgestellte Risiken.

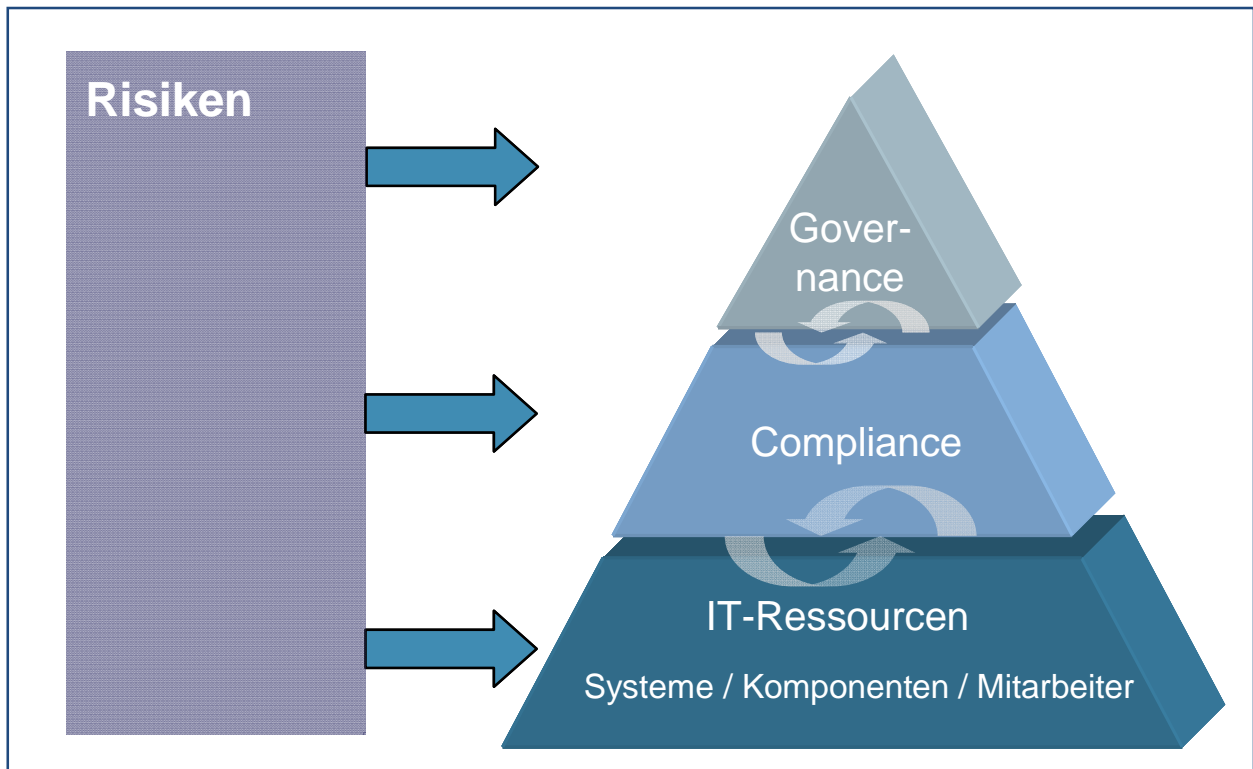


Abbildung 1: Zusammenspiel von Risiken, Governance und Compliance (eigene Darstellung).

Diese Studie beschäftigt sich nachfolgend primär mit dem Auslagern von IT-Infrastruktur und Geschäftsprozessen und den hierbei zu beachtenden Compliance-Vorgaben. Die sich daraus ergebenden Risikoaspekte und Governance-Vorgaben werden ebenfalls einbezogen, da es sich um ein kraftvolles Zusammenspiel dieser handelt.

3.2. IT-Outsourcing

3.2.1. Definition und Entwicklung

Der Begriff IT-Outsourcing ist weder in der theoretischen Literatur noch in der Praxis eindeutig definiert. Eine für diese Studie sinnvolle Abgrenzung beinhaltet folgende Bestandteile:

IT-Outsourcing bezeichnet die mittel- bis langfristige Übertragung von wesentlichen, aber nicht zu den Kernkompetenzen zählenden Teilen der gesamten IT-Infrastruktur bzw. der Auslagerung von ganzen Geschäftsprozessen mit ho-



hem IT-Anteil an einen spezialisierten, internen oder externen IT-Dienstleister, bei vorheriger Eigenerstellung der entsprechenden Aufgaben⁴.

IT-Outsourcing umfasst somit sowohl die Auslagerung von IT-Infrastrukturkomponenten (Rechenzentren, Netzwerke) und IT-Anwendungen (transaktionale und unterstützende Applikationen) als auch Geschäftsprozesse mit hohem IT-Anteil (Finanzwesen/Buchhaltung, Beschaffung). Die Auslagerung von Geschäftsprozessen ohne hohen IT-Anteil (Ausbildung/Training) oder andere Bereiche (z.B. Fuhrpark) sind in der Definition von IT-Outsourcing im Rahmen dieser Studie nicht inbegriffen.

Der erste große, in der Literatur bekannte Fall des IT-Outsourcing ereignete sich bereits 1963. Dabei übernahm der Outsourcing-Anbieter Electronic Data Systems (EDS) die komplette Datenverarbeitung des US-amerikanischen Krankenkassenzusammenschlusses Blue Cross und definierte damit einen neuen Markt [Hirschheim et al. 2004, S. 105]. Die Bedeutung des IT-Outsourcing nimmt seitdem mit kleineren Unterbrechungen ständig zu. Einen weiteren Meilenstein stellt der „IBM-Kodak Deal“ aus dem Jahr 1989 mit dem bis dahin höchsten Vertragsvolumen von ca. einer halben Milliarde US Dollar dar. Hohe Wachstumsraten bestätigen, dass auch nach der Jahrtausendwende die Bedeutung des IT-Outsourcing weiter steigt. [CIO 2007] Neuere Entwicklungen, die spätestens seit Beginn dieses Jahrtausends als etablierte Standards angesehen werden können, sind das Verlagern von Aufgaben in so genannte Niedriglohnländer, das Offshoring, aber auch das Auslagern ganzer Geschäftsprozesse, das so genannte Business Process Outsourcing (BPO).

In der wirtschaftswissenschaftlichen Forschung existieren verschiedene Erklärungsansätze für das Outsourcing. Bei der erstmals 1937 von Coase erwähnten **Transaktionskostentheorie** wird davon ausgegangen, dass eine Transaktion unter dem institutionellen Arrangement durchgeführt wird, das die geringsten Transaktionskosten verursacht. Der Transaktionskostentheorie folgend eignen sich daher besonders Standardleistungen und wenig spezifische, repetitive Aufgaben für ein Outsourcing.

⁴ In dieser Definition sind die wesentlichen Aspekte mehrerer in der Literatur gebräuchlicher Definitionen konsolidiert. Vgl. u.a.: [Behrens 2006, S. 6], [Knolmeyer 1998, S. 17], [Krcmar 2007, S. 371].

Die **Principal-Agent-Theorie** von Jensen und Meckling 1976 untersucht die Leistungsbeziehungen zwischen einem Auftraggeber (Principal) und einem Auftragnehmer (Agent). Dabei wird unterstellt, dass diese jeweils über unterschiedliche Informationsstände verfügen sowie voneinander abweichende Ziele verfolgen können. Aus diesem Zusammenspiel von Principal und Agent ergeben sich verschiedene mögliche Formen der Informationsasymmetrien bzw. Gefahren. Diese sind bspw. *Adverse Selektion* (Unvorteilhafte Auswahl eines Vertragspartners), *Hold Up* (Abhängigkeitseffekte) oder *Moral Hazard* (opportunistisches Ausnutzen von Handlungsspielräumen). Die Principal-Agent-Theorie liefert einen Erklärungsansatz für die Existenz verschiedener Organisationsformen des wirtschaftlichen Zusammenlebens. Es wird jeweils die Organisationsform gewählt, bei der die Auswirkungen der Informationsasymmetrien am geringsten sind bzw. bei der die möglichen Lösungen durch entsprechende Vertragsgestaltung am effizientesten umsetzbar sind. Liegt bei einer konkreten Outsourcing-Entscheidung eine potentielle Informationsasymmetrie des Typs „Hold Up“ vor, kann eine interne Lösung vorteilhafter als eine externe Lösung sein. Umgekehrt kann eine externe Lösung präferiert werden, wenn ein Unternehmen die Leistungsfähigkeit seiner Organisation in der konkreten Fragestellung nicht vollständig einschätzen kann. In einem solchen Fall könnte ein Outsourcing-Anbieter die Informationsasymmetrie durch den Nachweis seiner Leistungsfähigkeit (z.B. durch die Nutzung anerkannter Referenzmodelle oder sogar Zertifizierungen) abbauen.

Diese Theorien liefern die organisationstheoretische Grundlage für die Entscheidung bezüglich Outsourcing. In der unternehmerischen Praxis gibt es eine Reihe von Entscheidungsmodellen und -kriterien, auf der konkrete Entscheidungen für oder gegen ein Outsourcing basieren. Diese lassen sich in qualitative Modelle, wie *Argumentenbilanzen*, *Nutzwertanalysen* oder *Entscheidungsbäume*, und quantitative Modelle, wie Renditevergleichsrechnungen oder die Discounted Cash Flow-Methode (DCF), gliedern.

3.2.2. Formen des IT-Outsourcing

In der Literatur wie in der Unternehmenspraxis hat sich in den letzten Jahren eine Vielzahl unterschiedlicher Dimensionen des IT-Outsourcing etabliert. Im Folgenden wird IT-Outsourcing anhand der folgenden drei Dimensionen klassifiziert:



- Grad der Geschäftsorientierung (Leistungsform)
- Grad externer Leistungsbeziehung (Gestaltungsform)
- Grad der finanziellen Abhängigkeit (Organisationsform)

Durch den **Grad der Geschäftsorientierung** werden die Leistungsformen des IT-Outsourcing näher definiert. Der Bezeichnung entsprechend übernimmt bei *Infrastructure Outsourcing* ein interner oder auch externer Dienstleister die Wartung und den Betrieb der IT-Infrastruktur eines Unternehmens. Dazu zählen z.B. Router, Switches, Server, Drucker, Netzwerke, aber auch Betriebssysteme und Datenbanken. Beim *Application Outsourcing* wird das Anpassen an die betriebsindividuellen Anforderungen (customizing) und der Betrieb von Applikationen ausgelagert. Diese Form ist nicht mit dem *Application Service Providing (ASP)* zu verwechseln. Dabei werden die Anwendungen auf der Infrastruktur des Anbieters betrieben und den Kunden über Internet, Virtual Private Networks (VPN) oder andere Netze meist gegen eine nutzungabhängige Gebühr überlassen. Im Sinne des „1:n“-Ansatzes wird die Anwendung nicht an individuelle Anforderungen angepasst und steht vielen Unternehmen in gleicher Form zur Verfügung. Die Verantwortung über Lizenz, Wartung und Aktualisierung verbleibt beim Anbieter. *Business Process Outsourcing (BPO)* bezeichnet das Übertragen ganzer Unternehmensprozesse, in der Regel inklusive der prozessunterstützenden IT, an einen externen Dienstleister. Kerngeschäftsfremde und sich häufig wiederholende Prozesse, wie Einkaufsprozesse, Personalprozesse oder logistische Tätigkeiten, eignen sich besonders zum BPO.⁵

Der **Grad der externen Leistungsbeziehung** bestimmt, in welchem Umfang eine Auslagerung erfolgt. Die Klassifizierung von Outsourcing-Projekten nach Budget wird von Lacity und Willcocks (1995) vorgenommen. *Totales Outsourcing* liegt demnach vor, wenn mehr als 80 Prozent des Budgets an einen externen Dienstleister vergeben wurden. Sind zwischen 20 Prozent und 80 Prozent des Budgets ausgelagert, wird von *Selektivem Outsourcing*, Partiellem Outsourcing oder auch Outtasking gesprochen. Je nach Vorhaben des Outsourcing-Kunden kann eine bestimmte Gestal-

⁵ Zusätzlich zum klassischen BPO werden in der Praxis auch eine Reihe von Prozessen über mehrere Geschäftsfunktionen hinweg in einem einzigen, umfassenden Outsourcing-Projekt zusammengefasst, um größere Kosteneinsparungen und Wertsteigerungen schneller zu realisieren (Bundled Outsourcing).

tungsform vorteilhaft sein. Bei einem totalen Outsourcing lässt sich das auslagernde Unternehmen einerseits auf ein hohes Abhängigkeitsverhältnis mit dem Outsourcing-Anbieter ein. Andererseits besteht so die Möglichkeit, stärker von Kosten- und Qualitätsvorsprüngen des Dienstleister zu profitieren. Selektives Outsourcing eignet sich, wenn ein hohes Maß an Kontrolle und Flexibilität im Bezug auf das Outsourcing-Vorhaben notwendig ist.

Eine weitere Dimension stellt der **Grad der finanziellen Abhängigkeit** der beteiligten Partner bzw. die Organisationsform des Outsourcing dar. Allgemein werden dabei internes und externes Outsourcing bzw. Mischformen zwischen den beiden Reinformen unterschieden. *Internes Outsourcing* liegt bspw. vor, wenn Aktivitäten von unterschiedlichen Bereichen eines Unternehmens in einem internen Shared Service Center (SSC) zusammengezogen werden. Bei einem *externen Outsourcing* wird die Verantwortung an einen rechtlich und wirtschaftlich unabhängigen Partner ausgelagert. Ein Beispiel für eine Mischform ist ein *Joint Venture* zwischen Outsourcing-Kunde und Outsourcing-Anbieter.

Abbildung 2 stellt die bisher erläuterten Dimensionen im Zusammenhang dar.

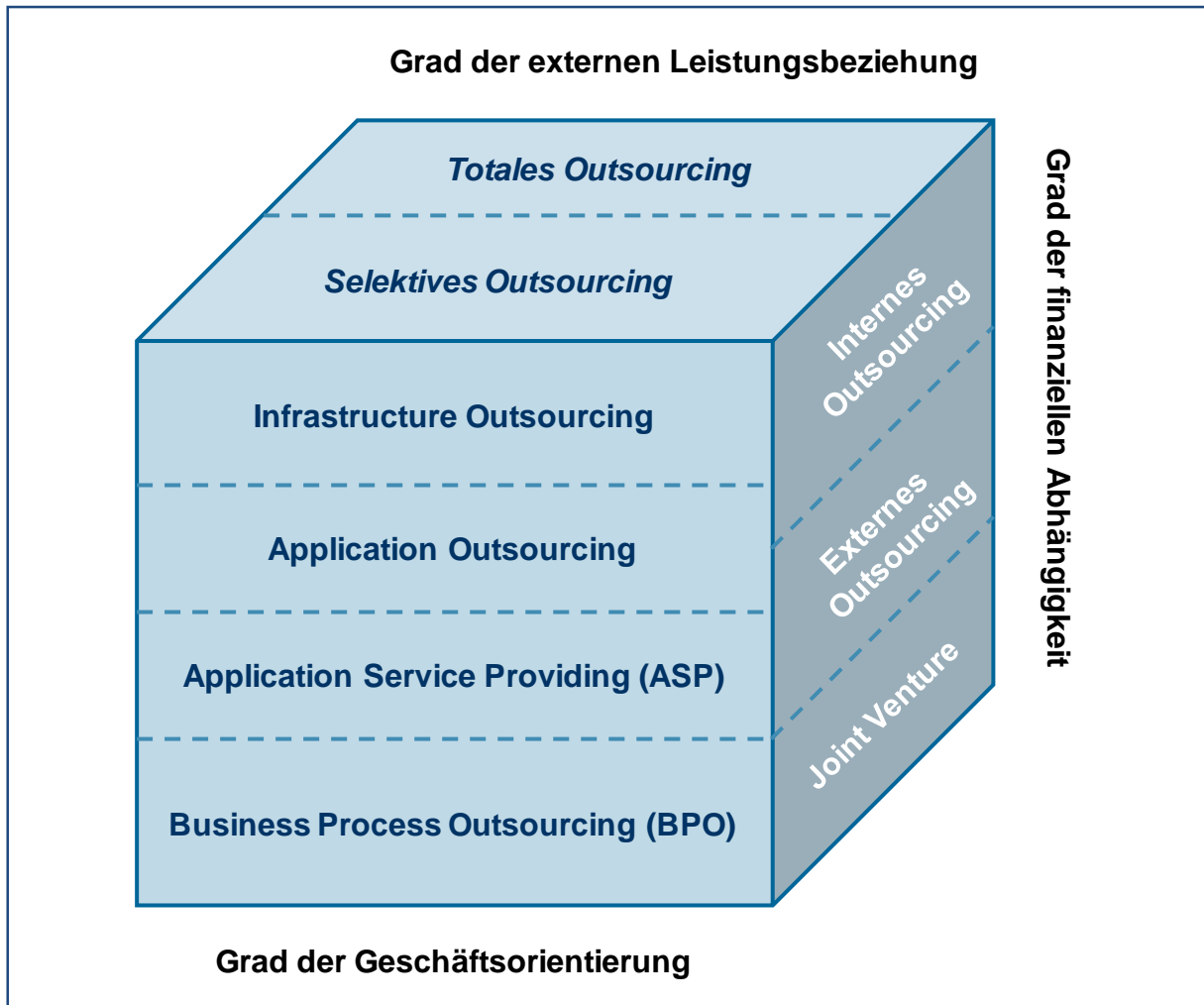


Abbildung 2: Klassifizierung von IT-Outsourcing (in Anlehnung an Amberg/Wiener).

Neben diesen drei Dimensionen gibt es eine Vielzahl weiterer Klassifizierungsmerkmale.

- So werden bspw. im Hinblick auf den Standort zumeist Offshoring, Nearshoring und Onshoring als mögliche Formen des Outsourcing unterschieden. Offshoring oder auch Offshore-Outsourcing bezeichnet das Auslagern in das entfernte Ausland, vornehmlich in so genannte Niedriglohnländer. Als Nearshoring wird aus zentraleuropäischer Sicht die Verlagerung von Aufgaben in Niedriglohnregionen innerhalb Europas (z.B. Slowakei, Rumänien) verstan-

den. Als Onshoring kann das Ansiedeln von ausgelagerten Aufgaben nahe des Produktionsstandorts im eigenen Land bezeichnet werden.

- Auch die Anzahl der Leistungserbringer ist ein mögliches Klassifizierungsmerkmal. Beim Multi- oder auch Multi-Vendor-Sourcing sind mehrere Leistungserbringer an einem Outsourcing-Projekt beteiligt. Der Vorteil dieser Methode liegt darin, dass für bestimmte Aspekte eines Outsourcing-Projekts der jeweils beste Anbieter beauftragt werden kann. Dieses wird auch als „best of breed“-Sourcing bezeichnet. Nachteile dieser Kooperationsform können durch Abstimmungsprobleme und mangelnde Kooperationsfähigkeit der Wettbewerber, aber auch durch Effizienzverluste durch fehlende Kompatibilität an den Schnittstellen entstehen. Im Gegensatz zu Multi-Sourcing bezeichnet Single-Sourcing die Beauftragung eines einzigen, Double-Sourcing zweier Anbieter für ein bestimmtes Projekt. Single-Sourcing hat vor allem bei Kooperationen mit externen Outsourcing-Anbietern den Vorteil, weniger Kontroll- und Abstimmungsaktivitäten, die sehr zeitintensiv sein können, vornehmen zu müssen, birgt aber die Gefahr einer Abhängigkeit.

3.2.3. Argumentenbilanz des IT-Outsourcing

Argumente für das IT-Outsourcing

Potentielle Kostenersparnisse sind beim IT-Outsourcing nach wie vor das wichtigste Argument. Dabei steht vor allem das Ausnutzen von Größenvorteilen (Skaleneffekte) im Vordergrund. Es wird angenommen, dass ein spezialisierter Dienstleister seine Leistungen in weit aus höheren Volumina herstellen kann als ein auslagerndes Unternehmen. Ressourcen können effizienter eingesetzt werden und Lerneffekte kommen früher zum Tragen. Die Stückkosten pro Leistungseinheit sinken. Hinzu kommt, dass bei Standardleistungen ein enormer Wettbewerbsdruck herrscht, der die Outsourcing-Anbieter zu größtmöglicher Rationalisierung zwingt und die Preise zusätzlich sinken lässt. Außerdem werden aus Sicht des Outsourcing-Kunden durch entsprechende leistungsabhängige Preisvereinbarungen fixe

Finanzielle Aspekte



Kostenblöcke flexibilisiert. Entscheidungsrelevante Informationen können aus der Entwicklung der Kosten leichter abgelesen werden. Die Planbarkeit und Zurechenbarkeit von Kosten wird verbessert. Die dadurch erreichte Kostentransparenz kann zu einem erhöhten Kostenbewusstsein in den betroffenen Abteilungen führen. In diesem Zusammenhang ist auch das verursachungsgerechte Vergütungsprinzip zu erwähnen. Dabei werden Leistungen von einem Kunden nur dann in Anspruch genommen (und damit kostenpflichtig), wenn sie tatsächlich gebraucht werden. Auch Aspekte der Rentabilität und Liquidität können wichtige Argumente für das Auslagern von Funktionen oder Geschäftsprozessen sein. Durch das Betreiben der IT innerhalb des eigenen Unternehmens werden erhebliche finanzielle Mittel gebunden. Wenn im Zuge eines Outsourcing Anlagevermögen an einen externen Dienstleister veräußert wird oder Ersatzinvestitionen für den Betrieb der IT vermieden werden können, wirkt sich diese Umwandlung von Anlagevermögen in laufende, voll absetzbare Aufwände positiv auf die Liquidität des Unternehmens aus. Außerdem lassen sich die frei werdenden Ressourcen einer rentableren oder strategisch wichtigeren Aufgabe zuführen.

Als wichtiger Hebel der strategischen Unternehmensführung wird seit Ende der 1990er Jahre die Konzentration auf das Kerngeschäft propagiert. Die Kernkompetenzen einer Organisation erfüllen mindestens folgende drei Bedingungen:

1. Sie leisten einen wesentlichen Beitrag zum wahrgenommenen Kundennutzen.
2. Sie sind schwer imitierbar.
3. Sie sind auf neue Produkte und Dienstleistungen übertragbar.

Funktionen, die nach dieser Logik nicht zu den Kernkompetenzen eines Unternehmens gehören, sollten daher ausgelagert werden. Dadurch werden Ressourcen frei, die in strategisch wichtigeren Un-

**Strategische
Aspekte**

ternehmensbereichen für den Aufbau langfristiger Wettbewerbsvorteile eingesetzt werden können. Ein Unternehmen, das sich auf seine Kernkompetenzen konzentriert und andere Funktionen von Dienstleistern erledigen lässt, erhöht die Flexibilität. Bei unerwarteten Veränderungen der Marktbedingungen können, bei entsprechender Vertragsgestaltung, Ressourcen flexibel auf- und abgebaut werden.

Outsourcing bietet die Möglichkeit, die Leistungsfähigkeit der Unternehmens-IT und/oder von Geschäftsprozessen zu optimieren. Üblicherweise werden Quantität und Qualität der ausgelagerten Dienstleistung durch vertragliche Service Level Agreements (SLA) klar definiert. Dadurch kann sich ein Outsourcing-Kunde vor schwankenden Qualitätsniveaus oder Lieferengpässen schützen. Außerdem lässt sich der zeitaufwändige und teure Aufbau von speziellem Know-how vermeiden. Durch die Zusammenarbeit mit spezialisierten Dienstleistern steht für bestimmte Projekte benötigtes Fachwissen punktgenau zur Verfügung. Verzögerungen, z.B. beim Eintritt in neue Märkte, beim Aufbau neuer Geschäftsfelder oder durch Schulung und Einarbeitung der eigenen Mitarbeiter entfallen, wodurch sich die „Time to Market“ beim Einführen neuer Produkte oder Dienstleistungen deutlich reduziert. Überdies werden betriebliche Abläufe eines Outsourcing-Kunden dadurch optimiert, dass ein spezialisierter Dienstleister „state-of-the-art“-Ausrüstung und -Prozesse bereitstellt, die er seinen Kunden als seine Kernkompetenz anbietet. Der Wettbewerbsdruck auf den Dienstleistungsmärkten zwingt die Anbieter darüber hinaus kontinuierlich zur Optimierung der Prozessqualität und zum Aufzeigen von Innovationsmöglichkeiten. Durch die Zusammenarbeit profitieren Outsourcing-Kunden von den hohen Qualitätsstandards der Outsourcing-Anbieter.

Leistungs- optimierung



Argumente gegen das IT-Outsourcing

Die Gefahr einer Abhängigkeit vom jeweiligen Partner wird häufig als eines der wichtigsten Argumente gegen das Outsourcing angesehen [Orange 2007]. Die meisten Outsourcing-Projekte sind auf eine langfristige Zusammenarbeit angelegt und daher – zumindest kurz- bis mittelfristig – nur unter sehr hohem Aufwand rückgängig zu machen. Unter Berücksichtigung der hohen Anlaufinvestitionen (bspw. Vertragserstellung, Service Transition, Outsourcing Due Dilligence, etc.), die ein Outsourcing-Kunde aufwenden muss, wird die Gefahr der Abhängigkeit vom (externen oder auch internen) Outsourcing-Anbieter umso deutlicher. Ein Wechsel bei unbefriedigenden Service Levels ist häufig auf Grund hoher Wechselkosten aus wirtschaftlicher Sicht unvorteilhaft.

Abhängigkeitseffekte

Nachdem potentielle Kostenersparnisse zu den größten Chancen des Outsourcing gehören, birgt – vice versa – die falsche Einschätzung der Einsparpotentiale ein hohes Risiko. Häufig werden bei der Analyse der Eigen- bzw. Fremderstellungskosten, die einer Outsourcing-Entscheidung zu Grunde liegt, wesentliche Kostenblöcke übersehen oder fehlerhaft bewertet. Als besonders anfällig für Fehleinschätzungen gilt die Transitionsphase. Bei Offshore-Projekten kann der finanzielle Aufwand für die Übergabe der Arbeiten an einen Dienstleister mit großer räumlicher und kultureller Distanz stark unterschätzt werden. Aber auch schon während der Anbahnungsphase können Fehler gemacht werden, die sich im weiteren Verlauf in höheren Gesamtkosten des Outsourcing niederschlagen.

Finanzielle Aspekte

Ein herausfordernder Aspekt beim Outsourcing an externe Dienstleister ist auch der mögliche Verlust von Know-how und eigener Innovationsfähigkeit. Hat ein Unternehmen weite Teile seiner Geschäftsprozesse oder Unternehmens-IT ausgelagert, so reduziert sich seine Fähigkeit, schnell auf neue Marktanforderungen zu reagie-

Verlust von Know-how und Innovationsfähigkeit

ren. Verstärkt wird diese Problematik beim Transfer von hoch spezialisiertem Personal zu einem externen Dienstleister. Dort stehen die Kenntnisse, je nach Vertragsgestaltung, möglicherweise auch anderen Kunden zur Verfügung. Die Auslagerung von Personal kann aber auch die emotionale Bindung an den bisherigen Arbeitgeber schwächen und bei Kündigung dieser Mitarbeiter zum Gesamtverlust des Know-how führen. Analog verhält es sich beim Wechsel des Outsourcing-Anbieters.

Nicht zu unterschätzen sind auch so genannte „weiche“ Faktoren⁶, die über Erfolg oder Misserfolg eines Outsourcing-Projekts entscheiden können. So spielt z.B. das Betriebsklima eine entscheidende Rolle. Selbst wenn eine Entscheidung für das Auslagern der Unternehmens-IT oder IT-naher Geschäftsprozesse und die damit verbundene Freisetzung von Personal aus wirtschaftlicher Sicht rational ist, heißt das nicht, dass die verbleibenden Mitarbeiter diese Ansicht teilen. Schon im Vorfeld einer Outsourcing-Entscheidung können Personalwiderstände zu erheblichen Problemen führen, bspw. wenn Mitarbeiter, die um Ihren Arbeitsplatz fürchten, in die Anbahnungs- oder Vereinbarungsphase eines Outsourcing-Projekts involviert sind und entscheidungsrelevante Informationen nicht oder fehlerhaft weitergegeben werden. Gerade beim Auslagern in Niedriglohnländer lässt die Angst vor organisatorischen Veränderungen oder Arbeitsplatzverlust häufig die Motivation und damit die Produktivität sinken.

„Weiche“ Faktoren

⁶ Mit „weichen“ Faktoren sind hier nicht unmittelbar monetär messbare Einflussgrößen wie z.B. Motivation, Betriebsklima oder die Bereitschaft der Zusammenarbeit mit Offshore-Kollegen gemeint.



Abbildung 3 fasst die Argumente für und gegen das IT-Outsourcing noch einmal zusammen und stellt diese in Form einer Argumentenbilanz gegenüber.

Argumentenbilanz des IT-Outsourcing			
Pro		Contra	
Finanzielle Aspekte	<ul style="list-style-type: none"> ▪ Kostenreduktion ▪ Fixkostenumwandlung ▪ Erhöhung von Rentabilität / Liquidität 	<ul style="list-style-type: none"> ▪ Opportunistisches Verhalten der Outsourcing-Partner ▪ Mittelfristig irreversibel 	Abhängigkeits-effekte
Strategische Aspekte	<ul style="list-style-type: none"> ▪ Konzentration auf das Kerngeschäft ▪ Flexibilität ▪ Verringerung der „Time to Market“ 	<ul style="list-style-type: none"> ▪ Fehleinschätzung Einsparpotentiale ▪ Hohe Kosten in der Transitionsphase ▪ Anpassungen der SLA 	Finanzielle Aspekte
Leistungs-optimierung	<ul style="list-style-type: none"> ▪ Stabile Qualitäts- / Quantitätsniveaus ▪ Zeitgenauer Zugang zu Know-how ▪ Zugang zu „state of the art“ -Ausrüstung / -Prozessen ▪ Optimierung der eigenen Prozesse 	<ul style="list-style-type: none"> ▪ Verlust von Know-how und/oder Innovationsfähigkeit ▪ Gefahr des Verpassens IT-basierter Trends 	Verlust von Know-how / Innovations-fähigkeit
		<ul style="list-style-type: none"> ▪ Motivationsprobleme beim verbleibenden Personal 	„Weiche“ Faktoren

Abbildung 3: Argumentenbilanz des IT-Outsourcing (eigene Darstellung).

Um den Argumenten gegen das IT-Outsourcing aktiv zu begegnen, sind daher die Auswahl und die Evaluierung des passenden Outsourcing-Anbieters sowie die vertraglichen Regelungen und deren operative Sicherstellung im Tagesgeschäft erfolgskritische Faktoren.

4. Rechtliche Rahmenbedingungen von Compliance und IT-Outsourcing

Um Compliance-Anforderungen zu genügen, müssen Unternehmen eine kaum zu überblickende Vielzahl an Anforderungen aus zum Teil sehr unterschiedlichen (Rechts-) Quellen erfüllen.⁷ Diese Zunahme an Anforderungen, insbesondere auf internationaler Ebene, sorgt bisweilen für große Ungewissheit. Immer häufiger werden wegen mangelnden Kenntnisstands externe Spezialisten in Projekte eingebunden, die teuer zugekauft werden müssen. Erschwerend kommt hinzu, dass Dienstleister (auch im Bereich des IT-Outsourcing) trotz zumeist vorhandenem Kenntnisstand keine Rechtsberatung und/oder Prüfung vornehmen dürfen.

Bei den Anforderungen, denen aus IT-Outsourcing-Geschichtspunkten Beachtung geschenkt werden muss, können neben **gesetzliche Regelungen** auch **Richtlinien, Standards und Referenzmodelle** sowie **innerbetriebliche Bestimmungen** unterschieden werden. Die überwiegende Zahl an gesetzlichen Regelungen gilt auch für die IT, selbst wenn diese nicht explizit im Gesetzestext erwähnt wird. So ist die IT sowohl mittelbar, wie durch die Forderung nach einem internen Kontrollsystem (IKS), als auch unmittelbar, wie durch das Bundesdatenschutzgesetz oder die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), betroffen [Heinze et al. 2005, S. 85]. Bei Richtlinien, Standards und Referenzmodellen handelt es sich um anerkannte Normen und „Best Practices“ ohne gesetzlichen Charakter, die jedoch Hilfestellungen zur Umsetzung von regulatorischen Vorgaben bieten. Auf die innerbetrieblichen Bestimmungen, wie einem „Code of Conduct“ im Rahmen der Corporate Governance oder spezifischen IT-Sicherheitsvorgaben, wird nachfolgend nicht näher eingegangen, da sie als individuelle Vorgaben häufig keine unternehmensübergreifende Anwendung zulassen. Arbeitsrechtliche sowie steuerrechtliche Aspekte werden im Rahmen dieser Studie nicht weiter verfolgt.

⁷ Unter Anforderungen werden sowohl nationale und internationale Gesetze als auch Richtlinien und Empfehlungen supranationaler Organisationen, die in nationales Recht umgesetzt werden, verstanden. Außerdem zählen zu ihnen Richtlinien und Standards, die über ihre Integration in gesetzliche Regelungen ihren Stellenwert erhalten oder Vorgaben, die als „state of the art“ (quasi) verbindliche Geltung besitzen.



4.1. Gesetzliche Regelungen

Im Folgenden werden Compliance-relevante gesetzliche Anforderungen auf ihre jeweiligen Implikationen für das IT-Outsourcing untersucht. Eine Ordnung der gesetzlichen Anforderungen nach ihrer Bedeutsamkeit ist hierbei nicht zielführend, da diese sehr unterschiedlich wirken und auch die Nichtbefolgung verschiedenartig geahndet wird. Allerdings stechen SOX und die 8. EU-Richtlinie (und in diesem Zusammenhang das geplante Bilanzrechtsmodernisierungsgesetz) durch ihre Medienpräsenz hervor.

Sarbanes-Oxley Act

Auf internationaler Ebene ist der Sarbanes-Oxley Act (SOX), der eine Reaktion auf diverse Bilanzskandale in der Vergangenheit darstellt, die wohl präsenteste gesetzliche Regelung. Die Vorschriften des SOX gelten für alle Unternehmen deren Wertpapiere in den USA gehandelt werden. Dazu können auch deutsche Unternehmen gehören.

Im Umfeld von SOX existieren im Wesentlichen zwei Publikationen des Public Companies Accounting Oversight Board (PCAOB), die den Umgang mit ausgelagerten Unternehmenseinheiten klären:

- In dem Board Release des PCAOB zum 2. Auditing Standard vom 9. März 2004 wird verdeutlicht, dass sich Unternehmen durch Auslagern nicht ihrer Verantwortung entziehen können. Dies bedeutet, dass Unternehmen auch dann in der rechtlichen Verantwortung für „ihre“ IT-Systeme und Prozesse verbleiben, wenn diese vollständig an einen externen Dienstleister übertragen werden. Daraus ergibt sich konsequenterweise, dass die auslagernden Unternehmen verbindliche Nachweise von ihren Dienstleistern fordern, dass diese über ein funktionierendes Kontrollsystem verfügen.
- Im Auditing Standard No. 5 des PCAOB wird auf SAS 70 - AU Section 324 „service organizations“ verwiesen. Dadurch wird die Vorgehensweise bei einer Prüfung geregelt, wenn Leistungen von einem Outsourcing-Anbieter bezogen werden, die zum IT-System des auslagernden Unternehmens zu zählen sind.

Section 324.03 listet Kriterien auf, nach denen solche fremdbezogenen Leistungen Teil des Informationssystems des auslagernden Unternehmens und damit Teil von dessen IKS sind. Die Bedeutung von SAS 70-Reports in diesem Zusammenhang wird in den PCAOB „Staff Questions and answers“ zusätzlich unterstrichen (siehe Abschnitt 0).

8. EU-Richtlinie und BilMoG

Die 8. EU-Richtlinie („Richtlinie 2006/43/EG über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen“) wird umgangssprachlich auch als „Euro-SOX“ bezeichnet. Gegenstand der Richtlinie ist die Harmonisierung der Anforderungen an die Abschlussprüfung innerhalb der EU [Lanfermann 2005, S. 2649]. Betroffene Unternehmen⁸ müssen ihre internen Kontrollen angemessen ausgestalten und Transparenz gewährleisten. Aus der 8. EU-Richtlinie ergibt sich somit, dass auch über Landesgrenzen hinweg ausgelagerte Dienstleistungen aus Compliance-Sicht im Verantwortungsbereich des auslagernden Unternehmens verbleiben. Das Gleiche gilt für Kontroll- und Qualitätssicherungssysteme.

Wesentliche Bestandteile der 8. EU-Richtlinie sollen in Deutschland durch das geplante Bilanzrechtsmodernisierungsgesetz (BilMoG) umgesetzt werden. Der gegenwärtige Gesetzesentwurf der Bundesregierung zum BilMoG stellt die umfangreichste Reform des deutschen Bilanzrechts seit über 20 Jahren dar. Das BilMoG definiert unter anderem die Zuständigkeit des Aufsichtsrats für die Wirksamkeit des IKS und des Risikomanagementsystems.

Handelsgesetzbuch

Das deutsche Handelsgesetzbuch (HGB) steht nicht direkt im Zentrum der aktuellen Compliance-Diskussion. Dennoch ist es im Compliance-Umfeld von Bedeutung, da sich hier verschiedene Compliance-Anforderungen konkretisieren bzw. daraus ableiten lassen. Für das Auslagern von Leistungen im Sinne des IT-Outsourcing ergeben

⁸ Unternehmen von öffentlichem Interesse mit einer Bilanzsumme von über 80 Mio. Euro (Dax-notierte Firmen, Banken, Versicherungen, Energieversorger oder Monopolunternehmen).



sich aus dem HGB diverse Anforderungen. Zentrale Norm ist § 238 HGB, der die Buchführungspflicht vorschreibt.⁹ Ist die Buchhaltung ganz oder teilweise ausgelagert, muss sichergestellt werden, dass auch das dafür beauftragte externe Unternehmen die Grundsätze ordnungsmäßiger Buchführung (GoB, vgl. Abschnitt 0) für das auslagernde Unternehmen einhält. Unterstützt wird diese Aussage durch § 238 Abs. 1 Satz 2 HGB und § 321 Abs. 1 HGB. In diesen wird die Gewährleistungspflicht vorgeschrieben, d.h. dass sich Dritte in angemessener Zeit ein klares Bild über die Geschäftsvorfälle machen können. Dies bestätigt die Notwendigkeit, die Einhaltung der GoB auch bei (externen) Dienstleistern zu kontrollieren.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist ein Artikelgesetz, das bestehende Gesetze, insbesondere HGB und AktG ändert bzw. ergänzt. Das KonTraG verpflichtet durch § 91 Abs. 2 AktG zur Einrichtung eines Risikomanagementsystems, in das auch Outsourcing-Anbieter eingebunden sein müssen. Korrespondierend dazu wurde in § 317 Abs. 4 HGB eine entsprechende Prüfungspflicht für Aktiengesellschaften aufgenommen. Der Wirtschaftsprüfer hat dabei zu beurteilen, „ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“

Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) ist nach § 3 Abs. 2 Satz 1 in jedem Fall anzuwenden, wenn die Datenverarbeitung automatisiert, also elektronisch durchgeführt wird.

Um Daten im Rahmen von Outsourcing weitergeben zu dürfen, muss zunächst ein gesetzlicher Erlaubnisstand nach § 4 Abs. 1 BDSG vorliegen. Hierbei stellt sich die Frage, welcher der Outsourcing-Partner für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist.

⁹ Die Buchführung muss „vollständig“, „richtig“, „zeitgerecht“, „geordnet“, „nachvollziehbar“ und „unveränderlich“ ausgestaltet sein (Vgl. §§ 238, 239 HGB).

Das BDSG unterscheidet zwei Formen der Übertragung von personenbezogenen Daten an Dritte: Auftragsdatenverarbeitung und Funktionsübertragung. Der dem Outsourcing zu Grunde liegende Vertrag bzw. eine Vertragsanlage sollte daher eindeutig klären, ob eine Auftragsdatenverarbeitung oder eine Funktionsübertragung vorliegt.¹⁰ Eine *Auftragsdatenverarbeitung* liegt vor, wenn es sich um die Wahrnehmung von reinen Unterstützungsfunktionen handelt. Hierbei verbleibt die Verantwortung beim auslagernden Unternehmen. Gehen die Leistungen über die reine Auftragsdatenverarbeitung hinaus, liegt eine *Funktionsübertragung* vor; die Verantwortung geht dann auf den Outsourcing-Anbieter über. Die Einwilligung nach § 4 Abs. 1 BDSG muss beim BDSG oder vom Betroffenen selbst zuvor eingeholt werden.

4.2. *Richtlinien, Standards und Referenzmodelle*

Neben den gesetzlichen Regelungen spielen Richtlinien, Standards und Referenzmodelle eine wichtige Rolle sowohl für Outsourcing-Kunden als auch Outsourcing-Anbieter:

- **Richtlinien** sind Handlungsanweisungen ohne direkten Rechtscharakter. Sie können aber von internationalen Organisationen (COSO) ausgegeben werden und haben somit einen bindenden und sanktionierbaren Charakter (in der Regel für bestimmte Zielgruppen). Hierbei müssen Richtlinien schriftlich fixiert und veröffentlicht werden.
- Bei einem **Standard** handelt es sich um eine Vereinheitlichung. Ein Standard ist ein Muster oder ein Vorgehen, das sich durchgesetzt hat. Standards haben grundsätzlich keinen verbindlichen Charakter, können aber verbindlich werden, wenn sie Teil einer Prüfung sind oder Bestandteil eines formalisierten oder nicht-formalisierten Regelwerks darstellen.
- Ein **Referenzmodell** ist ein allgemeines Muster, aus dem sich speziellere Ausprägungen (etwa Vorgehensweisen) ableiten lassen. Es lässt Vergleiche mit anderen Modellen zu und kann wieder verwendet werden, hat aber keinen verbindlichen Charakter.

¹⁰ Zu diesem Zweck stellt der BITKOM eine Mustervertragsanlage zur Auftragsdatenverarbeitung bereit.



Zusätzlich besteht die Möglichkeit, dass die Einhaltung von Richtlinien, Standards und Referenzmodellen von externen Gremien zertifiziert wird. Zertifikate eignen sich dazu, positive Signale über die Eigenschaften der zu zertifizierenden Funktionen an verschiedene Interessensgruppen zu senden oder schlichtweg die Erfüllung von Anforderungen nachzuweisen. Besonders für Outsourcing-Anbieter kann es von Vorteil sein, sich die Erfüllung bestimmter Standards zertifizieren zu lassen [Perdata 2008].

Basel II

Eine der wohl bekanntesten Richtlinien ist die Baseler Eigenkapitalvereinbarung (kurz Basel II). Im Zusammenhang mit Outsourcing werden zwei Wirkungen von Basel II unterschieden: die direkte (insbesondere relevant für Finanzinstitute) und die indirekte Einflussnahme.

Die direkte Einflussnahme von Basel II betrifft insbesondere die Behandlung von operationellen Risiken. Diese hängen direkt von der IT-Sicherheit ab und stellen nach allgemeiner Auffassung das zweitgrößte Verlustrisiko von Finanzinstituten dar [Lui 2005, S. 213]. Deshalb gelten besondere Regelungen, wenn geschäftskritische Prozesse ausgelagert werden. Die Anforderungen konkretisieren sich in § 25a Abs. 2 KWG. Danach muss ein Kreditinstitut je nach Art und Umfang seines Auslagerungsvorhabens geeignete Vorkehrungen treffen, um daraus entstehende übermäßige Risiken zu vermeiden. Weiterhin wird eindeutig bestimmt, dass die Verantwortung für die Einhaltung von gesetzlichen Bestimmungen beim auslagernden Unternehmen verbleibt.

Die indirekte Einflussnahme von Basel II auf andere Branchen macht sich bei der Kreditvergabe bemerkbar, da Finanzinstitute verstärkt auf das Kreditausfallrisiko ihrer Debitoren achten. Damit rücken auch deren ausgelagerte, geschäftskritische IT-Prozesse in den Fokus der Risikobetrachtung [BITKOM 2006, S. 30]. Um negative Auswirkungen auf die Bonität zu vermeiden, haben auslagernde Unternehmen ebenfalls ein Interesse, ihre Outsourcing-Anbieter zu überprüfen.

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

Eine weitere für das IT-Outsourcing relevante Richtlinie sind die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Sie bilden eine Verwaltungsanweisung des Bundesministeriums für Finanzen (BMF), deren rechtliche Grundlage die Abgabenordnung (AO) darstellt. Die GDPdU räumen der Finanzbehörde im Rahmen von steuerlichen Außenprüfungen das Recht zum Zugriff auf steuerrelevante Daten ein und regeln den Informationsaustausch zwischen Prüfer und Unternehmen. Diese müssen sicherstellen, dass alle steuerlich relevanten Daten identifiziert, vollständig und unverändert archiviert sowie unveränderbar gespeichert werden können [Kampffmeyer 2006, S. 6]. Weiterhin muss der Originalzustand der Daten erkennbar sein. Die GDPdU stehen in engem Zusammenhang zu den Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS – siehe nachfolgend) und fordern an mehreren Stellen bei der Umsetzung deren Berücksichtigung. Daher muss im Rahmen einer Prüfung sichergestellt sein, dass auch bei externen Outsourcing-Anbietern auf buchführungsrelevante Daten jederzeit zugegriffen werden kann.

Im Folgenden werden diverse **Standards** zur Behandlung ausgelagerter Unternehmens-IT und/oder kritischen Geschäftsprozessen (etwa Finanzwesen) vorgestellt. Durch die enge Verzahnung von IT und betrieblichen Abläufen haben diese eine hohe Relevanz. Dies betrifft insbesondere die Behandlung und Prüfung der Buchführung, da die Einhaltung von Richtlinien und Standards bei dem auftraggebenden, buchführungspflichtigen Unternehmen verbleibt. Aber auch begleitende Aspekte, wie zum Beispiel die Informationssicherheit, müssen von beiden Outsourcing-Parteien beachtet werden.



Grundsätze ordnungsmäßiger Buchführung

Die Grundsätze ordnungsmäßiger Buchführung (GoB) sind Standards zur Buchführung und Bilanzierung, die sich aus der Praxis der Buchführung, den Erkenntnissen der wissenschaftlichen Betriebswirtschaftslehre und der Rechtsprechung entwickelt haben und dabei teilweise in HGB und AO kodifiziert sind. Als wichtigste Grundsätze gelten:

- Formelle Richtigkeit, richtige Zeitfolge und Nachprüfbarkeit von Buchungen
- Klarheit der Buchführung
- Vollständigkeit und materielle Richtigkeit der Buchung von Geschäftsvorfällen
- Periodengerechte Abgrenzung von Buchungen
- Vorsicht bei der Bewertung von Vermögensgegenständen

Die Einhaltung der GoB liegt in der Verantwortung des Buchführungspflichtigen. Damit muss bei der Auslagerung von Buchhaltungsaufgaben das auslagernde Unternehmen die Einhaltung der GoB durch den Outsourcing-Anbieter kontrollieren.

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

Die Kernaussage der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) ist, dass auch bei DV-gestützter Buchführung die GoB eingehalten werden müssen. Die GoBS fordern ein Datensicherheitskonzept sowie präzise Anweisungen zur Dokumentation und Prüfbarkeit digitaler Daten.

Auch für die Einhaltung der GoBS ist der Buchführungspflichtige selbst verantwortlich [BITKOM 2006, S. 31]. Ist die IT-gestützte Buchführung ganz oder in Teilen ausgelagert, muss die Einhaltung der GoBS – analog zu den GoB – von der Geschäftsleitung nachweisbar sein. Darüber hinaus fordern die GoBS die Einrichtung eines IKS, was wiederum die Wichtigkeit von Überwachungsmaßnahmen bei IT-gestützten Prozessen zeigt. Zur Einrichtung eines IKS gemäß den Vorgaben der GoBS ist daher auch die Integration des Outsourcing-Anbieters in den Kontrollprozess notwendig.

Wirtschaftsprüfungsstandards (IDW PS 330 und IDW PS 951)

Die Standards des Instituts der Wirtschaftsprüfer in Deutschland (IDW) dokumentieren die vom Berufsstand der Wirtschaftsprüfer entwickelten Auffassungen und Regeln zur Berufsausübung. Zum Teil basieren sie auf internationalen Wirtschaftsprüfungsstandards oder entsprechen ihnen.

Mit dem Prüfungsstandard IDW PS 330 hat das IDW ein Standardprüfverfahren für Wirtschaftsprüfer zur „Abschlussprüfung bei Einsatz von Informationstechnologie“ herausgegeben [Nörr et al. 2005, S. 9].¹¹ Dabei wird festgelegt, wie die ausgelagerten Funktionen zu prüfen sind. Gemäß IDW RS FAIT 1 muss ein Unternehmen auch die Auswirkungen auf sein IKS beachten, wenn betriebliche (IT-) Funktionen ausgelagert werden. Dazu werden verschiedene mögliche Einflussfaktoren wie die Art der Outsourcing-Beziehung, die wirtschaftliche Lage, das IKS des Outsourcing-Anbieters sowie die Qualität der Kontrollen zur Überwachung der ausgelagerten Funktionen aufgezählt. Stuft der Prüfer die Aktivitäten des Outsourcing-Anbieters als wesentlich für die Abschlussprüfung ein, muss er sich um weitergehende Informationen zur Beurteilung von dessen IKS bemühen.¹² Eine entsprechende Bescheinigung über die Angemessenheit des IKS beim Outsourcing-Anbieter kann gemäß IDW PS 951 (siehe unten) ausgestellt werden.

Die Feststellung der Ordnungsmäßigkeit ausgelagerter Geschäftsprozesse und der damit verbundenen Unternehmens-IT ist somit ein wesentlicher Aspekt für Outsourcing-Kunden bei der Wahrnehmung ihrer betrieblichen Führungsverantwortung. Hierfür können Outsourcing-Anbieter international anerkannte Zertifizierungen als deutliches Zeichen für Verlässlichkeit und hohe Qualitätsstandards erwerben. Im Folgenden werden mit SAS 70 und dem deutschen Pendant IDW PS 331 zwei Zertifizierungen zur Prüfung unter anderem ausgelagerter Rechnungslegung vorgestellt.

¹¹ Die zu prüfende IT umfasst nach IDW RS FAIT 1 die IT-Infrastruktur, IT-Anwendungen und IT-gestützte Geschäftsprozesse.

¹² Eine Zertifizierung nach dem IDW PS 331 „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“ ist möglich.



Statement of Auditing Standard (SAS) 70

Die Statements of Auditing Standards des American Institute for Certified Public Accountants (AICPA) unterstützen (ähnlich der deutschen Standards des IDW) bei der Durchführung von Prüfungen. Das Statement of Auditing Standards Nr. 70 - **SAS 70** - gibt Dienstleistern analog zum IDW PS 951 die Möglichkeit, die Funktionsfähigkeit ihrer IKS anhand von zwei Varianten von Reports nachzuweisen:

- Der **Typ I-Report** beinhaltet lediglich beschreibende Aussagen über das Vorhandensein und den Aufbau eines IKS, nicht aber den Test von Kontrollmaßnahmen.
- Zum Nachweis von Compliance (z.B. zur SOX Section 404) ist ein **Typ II-Report** notwendig, da hier neben der Beschreibung des IKS durch Tests zusätzlich die Wirksamkeit und Effektivität der internen Kontrollen bzw. des gesamten IKS über eine Periode hinweg bestätigt werden.

Der SAS 70 hat für Outsourcing-Anbieter den Vorteil, dass dieser 1:n verwendet werden kann, d.h. dass ein SAS 70 Audit nur „einmal“ pro Outsourcing-Center durchgeführt werden muss und für unterschiedliche Kunden Anwendung findet. Zum Nachweis der Vorschriften des SOX wird in der Regel der SAS 70 Report verwendet. Der Ablauf von SAS 70 findet sich bei [Fröhlich et al. 2007a, S. 212-214].

IDW PS 331 / 951

Der IDW PS 331 „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“ konkretisiert die Prüfanforderungen des IDW PS 330 beim Outsourcing und gilt als deutsches Pendant zum SAS 70.

Zunächst muss die Art der Auslagerung des Rechnungswesens bestimmt werden. Führt ein Outsourcing-Anbieter vorgegebene Tätigkeiten nach direkter Anweisung des zu prüfenden Unternehmens durch, sind keine weiteren Maßnahmen nach **IDW PS 331** nötig. Führt er jedoch auftragsbedingt Handlungen eigenständig durch, muss der Prüfer die Auswirkungen dieser Handlungen auf das IKS des zu prüfenden Unternehmens beurteilen. Stellt dieser Interdependenzen fest, hat er zusätzliche Infor-

mationen einzuholen. Zum einen kann er dazu auf Prüfberichte eines externen Prüfers des Outsourcing-Anbieters zurückgreifen. Fällt diese Beurteilung positiv aus, kann eine Bescheinigung nach IDW PS 331 als Compliance-Nachweis für das IKS des Outsourcing-Anbieters verwendet werden [BITKOM 2006, S. 35]. Zum anderen kann der Abschlussprüfer zum Einholen zusätzlicher Informationen eigene Prüfhandlungen beim Outsourcing-Anbieter oder die Beauftragung eines externen Prüfers in Erwägung ziehen. Auch in diesem Fall muss der Bericht des Prüfers eine Funktionsprüfung des IKS beinhalten.

Der **IDW PS 951** mit dem Titel „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“ ergänzt den IDW PS 331. Darin wird erläutert, inwieweit sich Abschlussprüfer eines auslagernden Unternehmens auf die Berichte eines externen Prüfers über das IKS eines Outsourcing-Anbieters stützen dürfen. Der IDW PS 951 basiert auf den Anforderungen des SAS 70 und kann daher als eine Art Alternative mit Berücksichtigung nationaler Besonderheiten angesehen werden.

Der Nachweis erfolgt entweder mit einer „Typ A-Bescheinigung“, die ein Urteil des externen Prüfers über Darstellung und Angemessenheit des IKS beinhaltet, oder in Form einer „Typ B-Bescheinigung“, die zusätzlich mit Hilfe von Funktionsprüfungen die Wirksamkeit des IKS bestätigt (analog zu SAS 70).

Neben den bisher dargestellten Standards mit Fokussierung auf die ausgelagerte Rechnungslegung und deren Prüfung sind auch begleitende Aspekte, wie die *Informationssicherheit*, zu berücksichtigen. Im Folgenden wird dies anhand der Standards ISO 27001 und 27002 sowie des IT-Grundschutzhandbuchs exemplarisch vorgestellt.

ISO/IEC 27002 und 27001

Der ISO/IEC Standard 27002 „Information Technology – Code of Practice for Information Security Management“ (früher 17799) ist ein internationaler Standard, der Kontrollmechanismen für die Informationssicherheit beschreibt. Es werden Handlungsempfehlungen in 11 Überwachungsbereichen, u.a. dem Bereich „Compliance“,



gegeben und 134 diesen Bereichen zugeordnete Maßnahmen aufgezählt. Eine Zertifizierung nach ISO 27002 ist nicht möglich, da es sich um eine **Sammlung von „Best Practices“** und daraus abgeleiteten „Soll“-Forderungen und -Vorschlägen handelt.

Eine Zertifizierung des Informationssicherheitsmanagementsystems (ISMS) ist nach dem eng verbundenen ISO/IEC Standard 27001:2005¹³ mit dem Titel „Information Technology - Security Techniques - Informations Security Management Systems - Requirements“ möglich. Dieser Standard wurde von der ISA und der IEC erstmals im Herbst 2005 veröffentlicht und löst in seiner vollständig überarbeiteten Version den bisherigen British Standard BS 7799-2 ab. Die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten ISMS werden unter Bezugnahme auf die Kontrollen des ISO 27002 spezifiziert. ISO 27001 wurde entworfen, um die Auswahl geeigneter Sicherheitsmechanismen zum Schutz *sämtlicher IT-Komponenten* sicherzustellen. Unter Compliance-Gesichtspunkten bietet eine Zertifizierung nach ISO 27001 in IT-Outsourcing-Beziehungen eine Reihe von Vorteilen [Kersten 2008, S. 35 und 204 ff]:

- Identifikation der anwendbaren notwendigen Gesetze (Rechte, aber auch Pflichten aus Verträgen)
- Schutz geistigen Eigentums (Urhebergesetz)
- Schutz von bedeutenden Datensätzen und Dokumenten (SOX)
- Datenschutz- und Datensicherheit (BDSG)
- Zugangsschutz (SOX, KonTraG)
- Zugriffsschutz (GoBS, GDPdU, SOX)
- Regelungen zur Kryptografie (Verschlüsselungstechnik).

IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschreibt im Unterschied zum ISO 27001 Vorgehensweisen für Einzelmaßnahmen und lässt sich auch auf *einzelne IT-Anwendungen* beziehen.

¹³ Im Folgenden ISO 27001.

Das GSHB wird vom BSI kontinuierlich weiterentwickelt und hat sich an den ISO 27001 angenähert, so dass seit Anfang 2006 eine Zertifizierung nach ISO 27001 auf Basis des BSI-Grundschatzes möglich ist. Da sich viele Unternehmen in der Vergangenheit die Vorgehensweisen des IT-Grundschatzes zu Eigen gemacht haben, kann eine solche Zertifizierung nach ISO 27001 auch für Anbieter von IT-Outsourcing, die international operieren, dienlich sein. Besonders interessant ist für Outsourcing-Anbieter, dass beim IT-Grundschatz auch einzelne IT-Prozesse oder Fachaufgaben zertifizierbar sind. Vorteilhaft ist ebenfalls, dass explizit auf das BDSG als relevantes Gesetz eingegangen wird. Eine Zertifizierung nach BSI-Grundschatz signalisiert Outsourcing-Kunden ein hohes Niveau an Sicherheit. Allerdings gilt hier, dass die Prüfung der Ordnungsmäßigkeit des IKS durch einen Abschlussprüfer nicht ersetzt werden kann [BITKOM 2006, S. 35].

Abschließend werden in diesem Kapitel wichtige **Referenzmodelle** im Rahmen der zuvor beschriebenen Richtlinien und Standards im IT-Outsourcing vorgestellt: COSO, COBIT, ITIL und CMMI.

COSO

Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) ist eine privatwirtschaftliche US-amerikanische Organisation die Hilfestellungen bei der praktischen Gestaltung eines internen Kontrollsystems (IKS) gibt. Das gleichnamige COSO-Modell wurde 1992 publiziert und gilt heute insbesondere durch die Anerkennung der amerikanischen Börsenaufsicht SEC (Security Exchange Commission) als eines der führenden Referenzmodelle für IKS.¹⁴ Die Komponenten des IKS von COSO sehen wie folgt aus:

- **Kontrollumfeld:** Festlegung der globalen Kontrollziele, Aufbau der Compliance-Organisation, Richtlinien der Geschäftsführung
- **Risikobeurteilung:** Risikoidentifikation, Abstimmung mit dem Management, Kommunikation der erforderlichen Maßnahmen

¹⁴ Im Jahr 2004 hat COSO das COSO Enterprise Risk Management (ERM) veröffentlicht.



- **Kontrollaktivitäten:** Definition von Kontrollzielen und -tätigkeiten in der Organisation: Richtlinien, Prozeduren, Umsetzung der Anweisungen des Managements
- **Information und Kommunikation:** Informationsbereitstellung und Kommunikation an die Mitarbeiter zur Unterstützung ihrer Aufgabenerfüllung
- **Überwachung:** Überwachung und Verbesserung des implementierten Kontrollsystems sowie Nachhalten der Beseitigung von Abweichungen.

COSO hat den Schwerpunkt auf der Finanzberichterstattung und dient der Dokumentation, Analyse sowie Gestaltung des internen Kontrollsystems. IT-spezifische Vorgaben werden hier nicht gemacht.

COBIT

COBIT (Control Objectives for Information and Related Technology) ist ein Referenzmodell von weltweit akzeptierten und universell anwendbaren IT-prozessbezogenen Kontrollzielen (Control Objectives), die zum Erreichen von verlässlicher Anwendung der IT umgesetzt werden sollten [Gaulke 2006, S. 22]. COBIT hat die Intention bereits bestehende Standards wie die IT Infrastructure Library (ITIL)¹⁵ für Servicemanagement, ISO 27002 für Informationssicherheit oder ISO 9000 für Qualitätsmanagement zu integrieren [Goeken et al. 2006, S. 16] und vereint somit verschiedene Rahmenwerke. COBIT soll die Lücke zwischen allgemeinen und IT-spezifischen Kontrollmodellen schließen. COBIT definiert 34 IT-Prozesse mit über 300 Kontrollzielen.

Unter der Domäne „Planung & Organisation“ wird „Ensure Compliance with external requirements“ aufgeführt. COBIT berücksichtigt demnach auch Compliance-Anforderungen. Daher kann es sinnvoll sein, wenn beide Outsourcing-Parteien CO-

¹⁵ In der Theorie spielt die ITIL keine übergeordnete Rolle zur Herstellung von Compliance. Sie wird als Unterstützungsinstrument angesehen, aber nicht als Mittel, um speziell beim IT-Outsourcing Compliance herzustellen. Gründe der Divergenzen zwischen Theorie und Praxis könnten in der großen Verbreitung und dem Status der ITIL als „de-facto-Standard“ für IT-Service-Management in der Unternehmenspraxis liegen.

BIT für den Aufbau ihrer IT-Prozesse verwenden. [Huissoud] ist der Meinung, auch wenn sich Unternehmen nicht nach COBIT zertifizieren lassen können, sendet die Verwendung dieses Rahmenwerkes positive Signale an den jeweiligen Outsourcing-Partner [Huissoud 2001, S. 184]. COBIT ist ein von Wirtschaftsprüfern üblicherweise verwendetes IT-Prüfungsmodell. Outsourcing-Kunden können daher bei Befolgung von COBIT davon ausgehen, dass die wichtigsten Kontrollziele für die Prüfung des Outsourcing-Anbieters berücksichtigt wurden.

IT Infrastructure Library

Die IT Infrastructure Library (ITIL) ist ein international anerkanntes Referenzmodell für das IT-Servicemanagement. Es handelt sich um eine Sammlung von „Best Practice“ zur Ausgestaltung von Aufbauorganisation, effektiven Prozessen und Werkzeugen. Die Inhalte des Rahmenwerkes sind in der aktuellen Version ITIL V3 in fünf Büchern erfasst und orientieren sich an dem typischen Lebenszyklus von IT-Services: **Strategie, Entwurf, Betriebsüberleitung, Betrieb** und **Verbesserung**. Durch die Anwendung der ITIL lassen sich Risiken im IT-Umfeld (etwa Ausfallrisiko) besser managen. Außerdem wird eine Grundlage für IT-Sicherheit geschaffen, wie sie die steigenden gesetzlichen Anforderungen verlangen. Dennoch ergeben sich daraus weder eine allgemeine Verbindlichkeit noch spezifische Compliance-Anforderungen.¹⁶

In Outsourcing-Beziehungen ist die Verwendung der ITIL eine Möglichkeit zur reibungslosen und effektiven Zusammenarbeit. Durch die Standardisierung nach ITIL entsteht Wissen über Art und Aufbau der IT-Prozesse des jeweiligen Outsourcing-Partners, so dass Dienstleistungen besser und qualitativ hochwertiger erbracht und an die Bedürfnisse des Partners angepasst werden können. Die einheitliche Verwendung von Fachbegriffen und die Standardisierung von Prozessen trägt zum beiderseitigen Verständnis bei und lässt die Geschäftspartner „die gleiche Sprache“ sprechen. Auch die Einigung auf spezifische SLAs wird durch den Einsatz von Referenzmodellen wie ITIL bei beiden Outsourcing-Parteien erleichtert.¹⁷ Folgt ein

¹⁶ Vgl. Klotz (2007), S. 16.

¹⁷ Vgl. BSI (2005), S. 6.



Dienstleister den Empfehlungen der ITIL, kann er davon ausgehen, dass seine IT-Prozesse und damit auch die IT-Kontrollen auf einer gut strukturierten IT-Organisation aufbauen. Die Erfüllung der Anforderungen, die ein Outsourcing-Kunde an das IKS seines Outsourcing-Anbieters stellt, ist damit jedoch nicht garantiert und muss separat beachtet werden.

Capability Maturity Model Integration

Reifegradmodelle wurden entwickelt, um die Qualität von Prozessen¹⁸ zu beurteilen. Sie analysieren mit definierten Reifegradstufen, über welche Reife und Fähigkeiten das Analyseobjekt auf der betrachteten Analyseebene verfügt. Reifegradmodelle unterstützen und verbessern die Abläufe sowohl auf Projekt- als auch auf Unternehmensebene.

Mit der Capability Maturity Model Integration (CMMI) wird vom Software Engineering Institut (SEI) der US-amerikanischen Carnegie Mellon Universität ein zertifizierbares Referenzmodelle für die Produktentwicklung (insbesondere in der Softwareentwicklung), den Produkteinkauf und die Dienstleistungsentwicklung angeboten. Durch das CMMI werden aktuelle Praktiken kontinuierlich durch einen dynamischen Standard verbessert. Das CMMI besteht aus fünf Reifegraden. Diese dienen dazu, leicht verständlich die Prozessreife anhand eines Wortes oder einer Zahl zu beschreiben. Die fünf Reifegradstufen sind „Initial“, „Managed“, „Defined“, „Quantitatively Managed“ und „Optimizing“.

CMMI bietet sowohl für den Outsourcing-Kunden als auch den -Anbieter Vorteile. Letzterer kann seine internen Prozesse anhand eines international bewährten Referenzmodells formalisieren und auch zertifizieren lassen. Gerade diese Zertifizierungen sind für Outsourcing-Kunden ein deutliches Zeichen hoher und nachvollziehbarer Prozessqualität.

¹⁸ Unter einem Prozess wird die eindeutige Abfolge von Vorgängen, die notwendig sind, um ein Ziel zu erreichen, verstanden. Im Bereich der Software beinhaltet ein Prozess die Integration von Methoden, Aktivitäten und Veränderungen, die durchgeführt werden, um Produkte zu entwickeln, anzuwenden und zu pflegen.

5. IT-Outsourcing unter Compliance-Aspekten

In der Literatur werden Compliance-Aspekte bisher selten als Argumente für oder gegen das IT-Outsourcing genannt. So verbleibt Compliance in den Argumentationsbilanzen von [Hermes et al. 2005, S. 19], [Krcmar 2005, S. 273]; [Pallast 2002, S. 167], [Yang 2000; S. 230] oder [Knolmayer et al. 1998; S. 34] unberücksichtigt.

Aber auch in der Praxis scheint Compliance noch nicht den notwendigen Stellenwert erlangt zu haben. Beispielsweise waren gemäß einer Studie der MetaGroup aus dem Jahre 2007 25 Prozent von über 260 befragten Entscheidungsträgern nicht in der Lage zu sagen, welche Sourcing-Strategie als Reaktion auf SOX angebracht ist [Hall et al. 2007, S. 95 f.].

Aus diesem Grund werden nachfolgend die Pro- und Contra-Argumente von Compliance im IT-Outsourcing herausgearbeitet und evaluiert. Die klassischen Argumente für und gegen das IT-Outsourcing, wie in der Argumentenbilanz in Abschnitt 3.2.3 zusammengefasst, werden hier nicht noch einmal aufgegriffen.

5.1. Pro IT-Outsourcing

Aus der Sicht von Outsourcing-Kunden

Neben dem Standardargument der Kostensenkungspotentiale ist die Verbesserung der bisherigen Leistungen das wichtigste Argument für das Outsourcing. Im Hinblick auf Compliance liegen die Leistungsverbesserungen, die mit der Auslagerung an einen spezialisierten Dienstleister erzielt werden können, insbesondere im Bereich der formalisierten Abläufe und der Risikobeherrschung. Mögliche qualitative Leistungsverbesserungen ergeben sich zum einen durch die Formalisierung (und teilweise Standardisierung) operativer Tätigkeiten, wie Änderungsanträge oder Rollenvergaben. Derartige Maßnahmen senken auch das Compliance-Risiko, dass ungeplante Tätigkeiten den operativen Tagesablauf stören oder gar gefährden. Zum anderen verwenden Outsourcing-Anbieter zur Sicherstellung operativer Abläufe häufig eigene Erfahrungswerte sowie Steuerungs- und Überwachungsmaßnahmen, die wiederum die Prozesstransparenz beim Outsourcing-Kunden erhöhen und somit auch Risiko-



potentiale aufzeigen können. Zusätzlich lassen sich durch diese Prozesstransparenz auch Verbesserungspotentiale beim Outsourcing-Kunden aufzeigen.

Als weiteres Argument für IT-Outsourcing mit Hinblick auf Compliance können, neben den Kostensenkungspotentialen und einer Compliance-spezifischen Risikotransparenz, formalisierte Abläufe auch einen positiven Effekt auf die Unternehmensbewertung haben. Beispielsweise kann im Kontext von Basel II das Outsourcing von Leistungen von Vorteil sein, da Prüfungen des „operationellen Risikos“ häufig Bestandteil der Bonitätsprüfung sind, was sich letztendlich auch in den Kapitalkosten niederschlägt. Gerade bei mittelständischen Unternehmen ist anzunehmen, dass das Implementieren und Aufrechterhalten einer den Ansprüchen von Basel II genügenden IT-Sicherheit intern nur schwer zu bewältigen ist [Steria Mummert 2007]. Hier kann die Funktionsübertragung an einen professionellen Outsourcing-Anbieter das Risiko von höheren Kreditzinsen durch schlechtere Ratings verringern.

Vor dem Hintergrund der Realisierung einer wirksamen und wirtschaftlichen Governance für Geschäftsprozesse und Unternehmens-IT erscheint die Zusammenarbeit mit spezialisierten Dienstleistern eine gute Option. Dieses Vorgehen beinhaltet für das auslagernde Unternehmen die Möglichkeit, effektiver, schneller und kostengünstiger eine gute Governance zu erreichen [CGI 2005, S. 3 f.], um so neben den Kostensenkungspotentialen auch Risiken formalisiert und transparent anzugehen.

Aus der Sicht von Outsourcing-Anbietern

Für Outsourcing-Anbieter ergibt sich aus den verschärften Compliance-Anforderungen möglicherweise eine verstärkte Nachfrage nach dem bestehenden Leistungsangebot, da für viele Outsourcing-Kunden die selbständige Erfüllung aller Anforderungen nicht mehr möglich ist. Dabei können Outsourcing-Anbieter ihr Angebot anforderungs- oder auch zielgruppenspezifisch ausrichten und optimieren. Beispielsweise werden mittelständische Unternehmen, unter anderem um schlechtere Kreditkonditionen zu vermeiden, auf spezialisierte Dienstleister zurückgreifen müssen, da der hohe Mehraufwand (bspw. im Bereich der IT-Sicherheit) kaum noch alleine zu bewältigen ist.

Durch die Abdeckung von Compliance-Anforderungen wird es für Outsourcing-Anbieter auch möglich werden, Outsourcing-Kunden nicht nur durch Preis-, sondern auch durch Qualitätsargumente zu überzeugen. Dies dient als Abgrenzungsmerkmal in einem sich zunehmend verschärfenden Wettbewerb. Um den Qualitätsanspruch und die Vertrauenswürdigkeit der angebotenen standardisierten Abläufe zu belegen, können auch entsprechende Zertifizierungen (etwa CMMI) erworben werden.

Zusätzlich kann mit „neuen Leistungen“ dem Argwohn der Outsourcing-Kunden, für etwas verantwortlich zu sein, was sie nicht mehr im direkten Zu- bzw. Durchgriff haben, entgegenwirkt werden. Beispiele hierfür sind die durchgängige Analyse von Geschäftstransaktionen oder periodische Benchmarks.

5.2. Contra IT-Outsourcing

Aus der Sicht von Outsourcing-Kunden

Aus Sicht auslagernder Unternehmen ergeben sich aus den Compliance-Anforderungen deutliche Komplexitätssteigerungen, um den Verlust der eigenen Kontrollmöglichkeiten zu kompensieren (insbesondere bei externer Auslagerung). Der erhöhte Koordinationsaufwand steht dabei im Widerspruch zur Reduktion von Komplexität als Argument für das IT-Outsourcing. Regelungen wie der SOX, das KonTraG, Basel II, die 8. EU-Richtlinie, aber auch handelsrechtliche Vorschriften verpflichten auslagernde Unternehmen zu erhöhten Kontrollen ihrer Outsourcing-Anbieter. Darunter fallen die Kontrolle der Ordnungsmäßigkeit der Buchführung, die nachhaltige Überwachung und Kontrolle ausgelagerter IT-Funktionen sowie bilaterale Vertragsvereinbarungen. Darüber hinaus gilt (etwa bei SOX, dem KonTraG oder dem BilMoG), dass auch das IKS des Outsourcing-Anbieters als Bestandteil des IKS des Outsourcing-Kunden zu sehen ist und dementsprechend überprüft werden muss.

Ein weiteres, mögliches Argument gegen das IT-Outsourcing, das sich aus den Compliance-Vorschriften für auslagernde Unternehmen ergibt, liegt in der Haftungsfrage. Manager können für das Fehlverhalten von externen Dienstleistern zur Verantwortung gezogen werden. Damit müssen sie die Verantwortung für Handlungen übernehmen, die außerhalb ihres direkten Einflussbereichs liegen. Das steigert umso



mehr die Bedeutung der Auswahl renommierter Outsourcing-Anbieter, der Ausgestaltung entsprechender Vertragsbeziehungen und der Etablierung und kontinuierlichen Überwachung von Kontrollprozessen. Dies impliziert wiederum, dass ganz klare Anforderungen (Metriken und Controls) definiert werden müssen, die auch überprüfbar sind [Fröhlich et al. 2007a, S. 214]. Denn wenn ein Unternehmen seine Geschäftsprozesse oder IT auslagert, wächst die Abhängigkeit von einem Outsourcing-Anbieter und damit möglicherweise das Risiko, dass Compliance-relevante Vorschriften nicht ordnungsgemäß eingehalten werden. Dies kann sich aufgrund einer höheren Risikobeschaffenheit in einer höheren Risikoprämie und damit in den Kapitalkosten niederschlagen.

Aus der Sicht von Outsourcing-Anbietern

Für Outsourcing-Anbieter ergeben sich im Wesentlichen Nachteile durch Zusatzaufgaben, die übernommen werden müssen, um sowohl kundenspezifische Anforderungen abzudecken als auch sich weiterhin am Markt behaupten zu können.

Speziell in der initialen Transitionsphase steigert sich die Herausforderung der ohnehin komplexen und oft emotionalen Übernahmeprozesse, weil nun auch Compliance-relevante Aspekte identifiziert und in den Gesamtprozess integriert werden müssen. Dies spiegelt sich in immer komplexeren Vertragskonstrukten wieder. Im weiteren Verlauf des Outsourcings erhöht sich häufig der Mehraufwand um die Kontroll-, Überwachungs- und Nachweisanforderungen der Outsourcing-Kunden befriedigen zu können.

Zusätzlich werden am Markt anerkannte Zertifikate gefordert, was kontinuierlicher Investitionen in Mitarbeiter, Prozesse und Technologien bedarf.

Teil 2



6. Empirische Untersuchung

Um die in den vorangegangenen Kapiteln erarbeiteten Ergebnisse zu bewerten und einzuordnen, wurde vom Lehrstuhl für Wirtschaftsinformatik III der Friedrich-Alexander-Universität Erlangen-Nürnberg 2008 eine anonymisierte Expertenumfrage mit dem Titel „Compliance Aspekte im IT-Outsourcing“ durchgeführt. Ziel war es, durch die Befragung möglichst vieler Experten aus den Fachgebieten IT-Outsourcing¹⁹ und/oder Compliance ein aussagekräftiges Meinungsbild aus der Praxis über die Zusammenhänge von IT-Outsourcing und Compliance zu erhalten.

Stichprobengröße: 233 Teilnehmer (N=233), von denen 56 Prozent (n=132) die Online-Befragung beendeten.

Rekrutierungstechniken: Die Probanden wurden mit Hilfe von virtuellen sozialen Netzwerken, Internetrecherchen und persönlichen Kontakten identifiziert und rekrutiert.

Unternehmen: Die Antworten kamen mit jeweils etwa 40 Prozent größtenteils von Beschäftigten aus GmbHs und AGs. Knapp die Hälfte der involvierten Unternehmen hatte 2000 oder mehr Mitarbeiter, weitere 20 Prozent zwischen 500 und 2000 Mitarbeiter.

Branchen: Mit über 40 Prozent kamen die meisten Probanden aus der IT-Branche, gefolgt von der Beratungsbranche mit etwa 20 Prozent und der Finanzdienstleistungsbranche mit etwa 15 Prozent. Branchen mit einem Anteil größer fünf Prozent waren Automobil- und Pharma-/Gesundheitsbranche.

Teilnehmerkreis: Über 60 Prozent der Teilnehmer sind in höheren Managementpositionen tätig oder haben eine leitende Funktion in IT- oder Finanzabteilungen.

Im Mittelpunkt der empirischen Untersuchung stand die Fragestellung, ob Compliance als Argument für oder gegen das IT-Outsourcing berücksichtigt werden muss. Untersucht wurden:

¹⁹ Unter dem Begriff IT-Outsourcing wurde sowohl das Infrastruktur- und Applikations-Outsourcing als auch das Auslagern von Geschäftsprozessen (Business Process Outsourcing) verstanden.

- Relevante Gesetze für das IT-Outsourcing
- Rahmenwerke, Zertifikate und Standards beim IT-Outsourcing
- Compliance als Argument pro oder contra IT-Outsourcing.

Die Auswertung und Analyse der Antworten erfolgte aus verschiedenen Blickwinkeln: aus Sicht **aller Parteien**, aus Sicht von **Outsourcing-Kunden** und aus Sicht von **Outsourcing-Anbietern**.

6.1. Relevante Gesetze für das IT-Outsourcing

Frage: Welche Regelungen/Gesetze sind für die befragten Unternehmen im Zusammenhang mit IT-Outsourcing relevant?

Die wichtigste *externe* Vorgabe ist für die befragten Unternehmen der Sarbanes-Oxley Act (SOX). 46 Prozent stufen ihn als „sehr wichtig“ ein. Danach folgen das BDSG, Basel II und das KonTraG. Die Vorgaben der 8. EU-Richtlinie werden von den Befragten bisher noch nicht zu den sehr wichtigen Regelungen mit Auswirkungen auf das IT-Outsourcing gezählt. Eine bedeutende Rolle spielen auch *interne* Richtlinien. Knapp 62 Prozent der Befragten beurteilten diese als „sehr wichtig“.

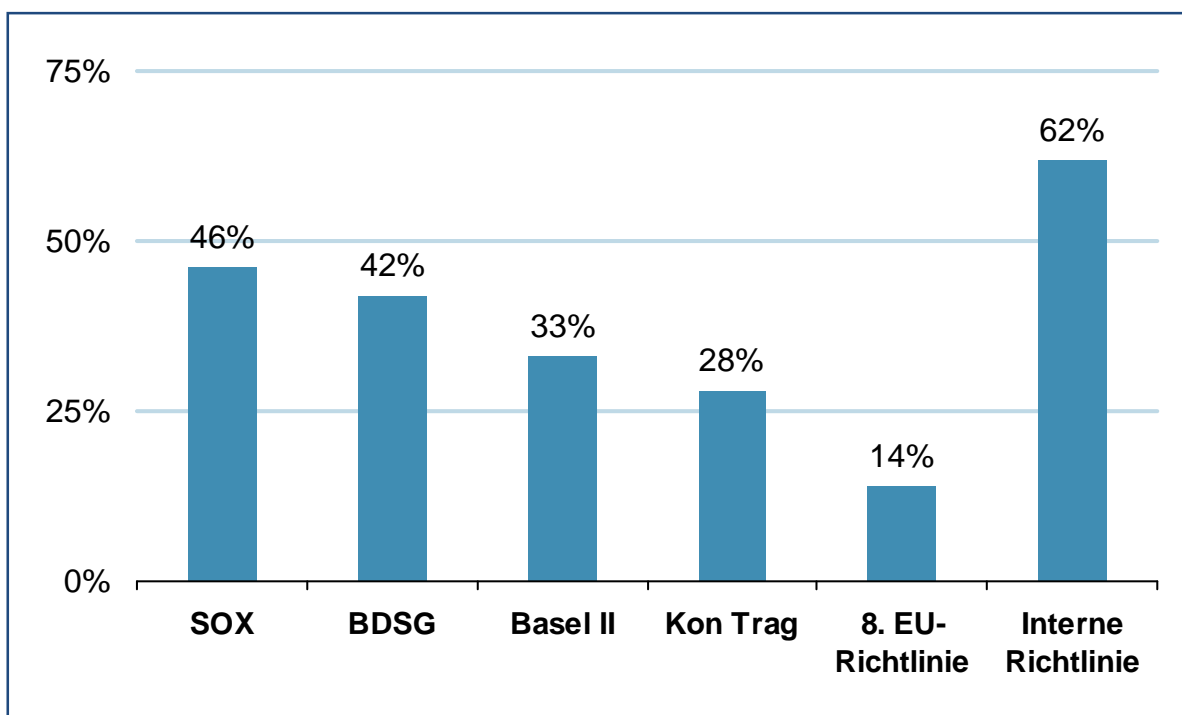


Abbildung 4: IT-Outsourcing relevante Regelungen (eigene Darstellung).



Abbildung 4 verdeutlicht die zuvor erläuterten Antworten und zeigt auf, wie viel Prozent **aller Teilnehmer** die jeweiligen Regelungen als „sehr wichtig“ eingestuft haben. Weitere Antwortoptionen waren „wichtig“ und „nicht relevant“.

Interessant ist auch die Auswertung zur Relevanz von Basel II: Befragte, die aus Sicht von **Outsourcing-Kunden** antworteten, sahen zu 52 Prozent Basel II als sehr wichtig an, **Outsourcing-Anbieter** zu etwa 26 Prozent, obwohl nur 15 Prozent der Befragten aus der Finanzdienstleistungsbranche kommen. Dies zeigt, dass Outsourcing-Kunden außerhalb der Finanzdienstleistungsbranche den Einfluss der Basel II-Vorschriften auf ihre Finanzierungsoptionen und -kosten (Bonität) Beachtung schenken. Damit rücken auch ausgelagerte, geschäftskritische IT-Prozesse in den Fokus der Risikobetrachtung.

6.2. Rahmenwerke, Zertifikate und Standards beim IT-Outsourcing

Internationale Rahmenwerke, Standards und Zertifikate haben sich als wichtige Mittel zum Nachweis von Compliance in IT-Outsourcing-Beziehungen etabliert. Besonders bedeutsam in diesem Zusammenhang ist der SAS 70-Report, der im SOX-Umfeld als Quasi-Standard zum Nachweis von „Sektion 404“ (Interne Kontrolle der Finanzberichterstattung) gilt. Folglich gaben auch etwa 70 Prozent **aller Unternehmen**, die SOX als sehr wichtiges Gesetz im Zusammenhang mit IT-Outsourcing sahen, an, dass sie SAS 70-Reports erstellen bzw. verlangen. Laut Umfrage ist der SAS 70-Report vor allem für **Outsourcing-Anbieter** relevant: Etwa die Hälfte der Befragten gaben an, SAS 70-Reports zu erstellen.

Rahmenwerke und Referenzmodelle wie die IT Infrastructure Library (ITIL) oder die Control Objectives for Information and Related Technology (COBIT) sind in den befragten Unternehmen, die den Compliance-Anforderungen gerecht werden, auch für das IT-Outsourcing von Bedeutung. So gaben über 55 Prozent **aller Befragten** an, dass COBIT in ihrem Unternehmen im Zusammenhang mit IT-Outsourcing eine Rolle spielt. Bei ITIL war dies sogar bei mehr als drei Viertel der Teilnehmer der Fall.

6.3. Compliance als Argument pro oder contra IT-Outsourcing

Um der Frage auf den Grund zu gehen, ob Compliance als Argument bei IT-Outsourcing-Entscheidungen berücksichtigt werden muss, wurde zweistufig vorgegangen. Zunächst sollte die allgemeine Bedeutung von Compliance für IT-Outsourcing-Entscheidungen herausgearbeitet werden. Im zweiten Schritt wurden die Teilnehmer gebeten, konkret dazu Stellung zu nehmen, wie und ob Compliance Outsourcing-Entscheidungen in ihren Unternehmen beeinflusst.

6.3.1. Allgemeine Bedeutung von Compliance für IT-Outsourcing-Entscheidungen

Beurteilung der Aussage „Compliance spielt bei IT-Outsourcing-Entscheidungen eine wichtige Rolle.“

Diese Aussage bewerteten 57 Prozent **aller Teilnehmer** mit „stimme zu“ und 30 Prozent mit „stimme eher zu“. Dabei ist, wie Abbildung 5 verdeutlicht, insbesondere bei **Outsourcing-Anbietern** Compliance ein wichtiger Aspekt bei IT-Outsourcing-Entscheidungen. Von ihnen stimmten 56 Prozent uneingeschränkt zu, während es bei den **Outsourcing-Kunden** 41 Prozent waren.

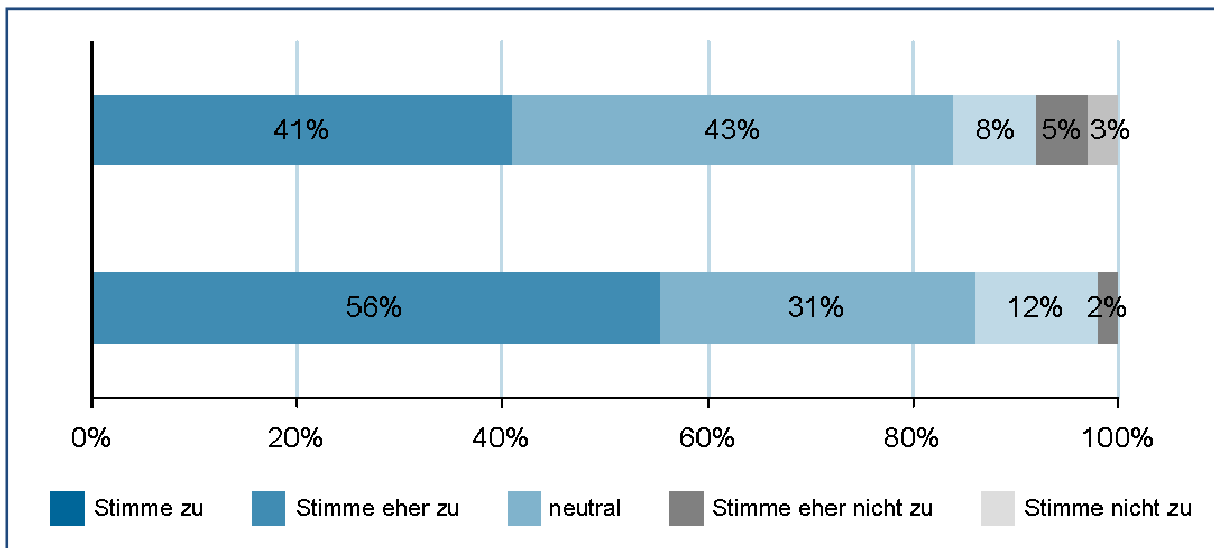


Abbildung 5: Beurteilung der Aussage „Compliance spielt bei IT-Outsourcing-Entscheidungen eine wichtige Rolle“ (eigene Darstellung).



Lediglich bei etwa drei Prozent aller Teilnehmer spielt Compliance keine Rolle für IT-Outsourcing-Entscheidungen. Für eine deutliche Mehrheit ist Compliance also ein wichtiger Faktor bei IT-Outsourcing-Entscheidungen.

6.3.2. Einfluss von Compliance Anforderungen bei konkreten IT-Outsourcing-Entscheidungen

Frage: Haben Compliance Anforderungen schon einmal negativen Einfluss auf konkrete Outsourcing-Entscheidungen genommen?

Bei rund 40 Prozent **aller Unternehmen** haben Compliance-Anforderungen bereits einmal negativen Einfluss auf konkrete Outsourcing-Entscheidungen genommen.

Bei differenzierter Betrachtung ist Compliance vor allem bei börsennotierten Unternehmen mit mehr als 2000 Mitarbeitern, die als **Outsourcing-Kunden** auftreten, ein Hinderungsgrund für das IT-Outsourcing. Bei einzelnen Entscheidungssituationen, in denen Argumente aus Compliance-Sicht gegen das Auslagern sprechen (z.B. erhöhte Anforderung an interne Kontrollen, Managerhaftung für Handlungen von IT-Dienstleistern, die außerhalb des direkten Einflussbereiches liegen oder stärkere Kontrollpflichten beim IT-Dienstleister), wurden diese höher bewertet als die potentiellen Vorteile. Dieses Ergebnis ist vor dem Hintergrund, dass Compliance als Gegenargument in den gängigen Entscheidungsmodellen kaum berücksichtigt wird, besonders hervorzuheben.

Frage: Haben Compliance Anforderungen bereits Outsourcing-Entscheidungen unterstützt?

Auf diese Frage antworteten etwa 40 Prozent **aller Befragten** mit „ja“. Diese positiven Antworten kamen überwiegend von großen Aktiengesellschaften. Dabei lag der Anteil der **Outsourcing-Anbieter** bei 60 Prozent gegenüber einem Anteil von **Outsourcing-Kunden** von nur 35 Prozent. Die Diskrepanz zwischen Outsourcing-Anbieter und -Kunden zeigt zum einen, dass Outsourcing-Anbieter Compliance als Vorteil im Entscheidungsprozess für IT-Outsourcing sehen. Zum anderen lässt sich bei Outsourcing-Kunden auf die Sensibilität dieses Themas schließen.

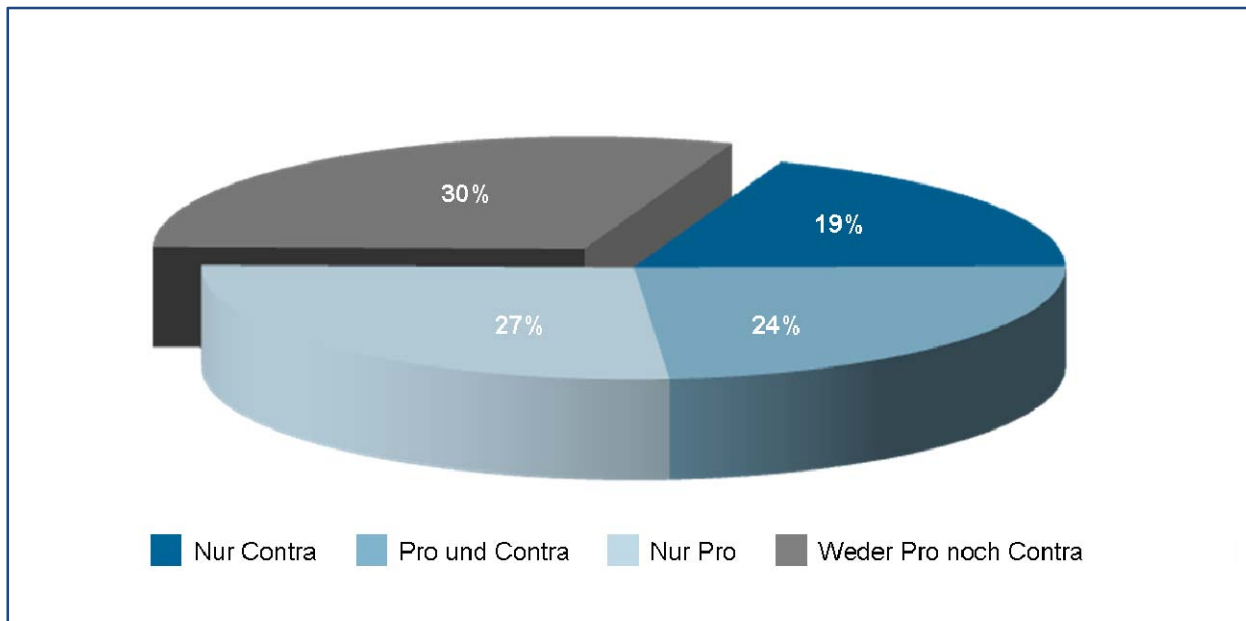


Abbildung 6: Compliance als Pro- bzw. Contra-Argument beim IT-Outsourcing (eigene Darstellung).

Abbildung 6 fasst die Ergebnisse der Fragen nach Compliance als Pro- und Contra-Argument zusammen. Bei mehr als zwei Drittel der Befragten hatten Compliance-Aspekte bereits Auswirkungen auf IT-Outsourcing-Entscheidungen (Pro oder Contra). Davon war bei etwa 24 Prozent Compliance sowohl ein Pro- als auch ein Contra-Argument für das IT-Outsourcing; bei 27 Prozent wurde Compliance nur als Argument „dafür“, bei 19 Prozent nur „dagegen“ angeführt. Demnach führten nur 30 Prozent Compliance weder als Pro- noch als Contra-Argument an.

Auf Basis dieser Umfrageergebnisse sollte Compliance in Zukunft als eigenständiges Argument in Entscheidungsmodellen zum IT-Outsourcing berücksichtigt werden.

Frage: Erhöhen Compliance Anforderungen die Kosten des IT-Outsourcing?

Da die finanziellen Aspekte im Zusammenhang mit IT-Outsourcing-Entscheidungen eine besonders wichtige Rolle einnehmen, wurden die Teilnehmer gefragt, ob aus ihrer Sicht Compliance-Auflagen die Kosten des IT-Outsourcing erhöhen. Auch diese rein monetäre Betrachtung der Zusammenhänge von IT-Outsourcing und Compliance ergibt ein eindeutiges Bild: Nach Auffassung von 82 Prozent der **Outsourcing-Anbieter** wird das IT-Outsourcing durch Compliance-Vorgaben kostenintensiver.

Aber auch für zwei Drittel der **Outsourcing-Kunden** trägt Compliance zu höheren Kosten im IT-Outsourcing bei. Abbildung 7 verdeutlicht die Einschätzungen der Befragten.

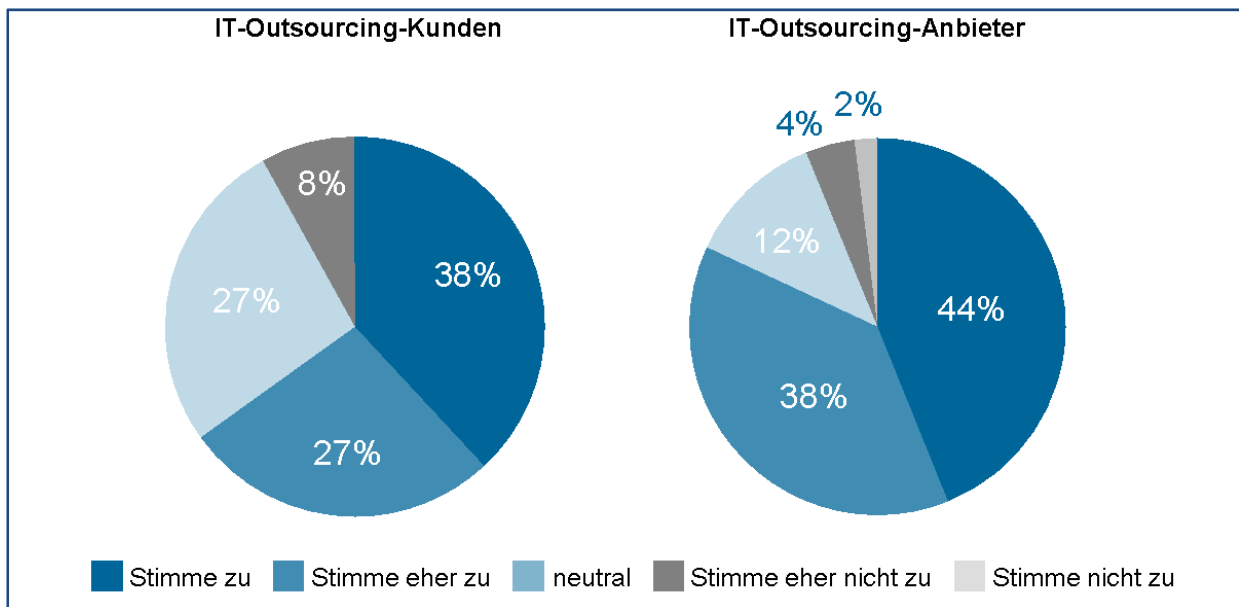


Abbildung 7: Beurteilung der Frage „Erhöhen Compliance Anforderungen die Kosten des IT-Outsourcing?“ (eigene Darstellung).

Wie die Analyse der relevanten Vorschriften in Kapitel 4 gezeigt hat, bleibt die Verantwortung für die Erfüllung der meisten Compliance Anforderungen beim auslagernden Unternehmen. Compliance-Nachweise müssen dennoch beim Outsourcing-Dienstleister eingeholt werden.

Frage: Machen Compliance Vorgaben das Outsourcing weniger attraktiv?

Diese Aussage wurde von knapp einem Drittel **aller Befragten** bejaht. Demgegenüber spielt bei etwa 45 Prozent Compliance keine bzw. nur eine geringe Rolle für die Attraktivität des IT-Outsourcing. Bei näherer Betrachtung fällt auf, dass für diese Unternehmen Referenzmodelle und vor allem Zertifikate wie BSI-Grundschutz oder ISO 27001 besonders wichtig waren. Das lässt darauf schließen, dass die Nachteile, die aus Compliance-Anforderungen für das IT-Outsourcing entstehen, durch Anwendung von Standards und Referenzmodellen wie COBIT, ITIL, ISO 27001, oder auch SAS 70-Reports abgeschwächt werden können.

7. Compliance in der Outsourcing-Praxis

Zur Validierung der theoretischen Erkenntnisse und der quantitativen Analysen wird nachfolgend die zunehmende Bedeutung von Compliance anhand eines konkreten Outsourcing-Projekts unterstrichen sowie Maßnahmen zur konkreten Beachtung von Compliance in der Praxis durch Accenture dargestellt.

7.1. Accenture – das Unternehmen

Accenture ist ein weltweit agierender Managementberatungs-, Technologie- und Outsourcing-Dienstleister. Rund 186.000 Mitarbeiter in 52 Ländern sorgen mit umfassendem Branchenwissen dafür, Projekte und Dienstleistungen für Kunden in über 120 Ländern erfolgreich zu realisieren. Zu diesen Kunden zählen weltweit über 4.000 Organisationen. Dazu gehören 96 Unternehmen aus dem Fortune-Global-100-Index sowie mehr als drei Viertel der im Fortune Global 500 aufgelisteten Organisationen.

Zu einem wichtigen Bestandteil des Accenture-Portfolios hat sich in den vergangenen Jahren das Geschäftsfeld der Outsourcing-Dienstleistungen entwickelt. Seit mehr als 15 Jahren bietet Accenture Dienstleistungen in diesem Bereich an und konnte über 600 Outsourcing-Projekte für führende Unternehmen und Regierungseinrichtungen aus mehr als 75 Ländern durchführen. Das Accenture Outsourcing-Portfolio umfasst die folgenden vier Kernbereiche:

- **Infrastructure Outsourcing** (Outsourcing von IT-Infrastruktur) befähigt Unternehmen, die Flexibilität, Skalierbarkeit, Zuverlässigkeit und Sicherheit ihrer IT-Infrastruktur zu verbessern und beinhaltet etwa Arbeitsplatz-, Netzwerk- und Rechenzentrums-Dienstleistungen, IT-Sicherheit oder Management der IT-Ausgaben.
- **Application Outsourcing** (Outsourcing von IT-Anwendungen) umfasst beispielsweise die Verantwortungsübernahme für den langfristigen Betrieb einzelner IT-Anwendungen oder eines bestehenden IT-Anwendungsportfolios, die ganzheitliche Konzeptionen sowie die Steuerung und Durchführung von definierten Testzyklen oder die Entwicklung von Individuallösungen für die jeweilige Unternehmenssoftware.

- **Business Process Outsourcing** (Outsourcing von Geschäftsprozessen) ist die Übernahme der Verantwortung für einzelne oder auch mehrere Geschäftsprozesse, beispielsweise im Finanz- und Rechnungswesen, Personalwesen, Einkauf, Kundenbetreuung aber auch branchenspezifische Lösungen.
- **Bundled Outsourcing** (Gebündeltes Outsourcing von mehreren Geschäftsprozessen) fasst eine Reihe von Prozessen über mehrere Geschäftsfunktionen hinweg in einem einzigen, umfassenden Outsourcing-Projekt zusammen, wie Prozesse des Finanz- und Rechnungswesen kombiniert mit Prozessen des Personalwesens.

Mit dem Accenture Delivery Network, einem Netzwerk von Dienstleistungszentren, ist Accenture ein Pionier in der Industrialisierung der Informationstechnologie und des Geschäftsprozessumfeldes. Jedes der über 50 Delivery Center ist mit der modernsten Informationstechnologie ausgerüstet und agiert in dem globalen Netzwerkverbund. Aufgrund der sorgfältigen Auswahl der Standorte kann Accenture jeden Service 24 Stunden am Tag und 7 Tage die Woche zur Verfügung stellen. In jedem Delivery Center arbeiten Fachleute für verschiedene Geschäftsprozesse bzw. für nahezu jede technische Problemstellung. Darüber hinaus stehen die Dienstleistungen in über 20 Sprachen zur Verfügung.



Abbildung 8: Accenture Delivery Network (eigene Darstellung).

Die Nutzung weltweit konsistenter Prozesse und Technologien im Accenture Delivery Network stellt eine geografie- und geschäftsübergreifend gleich bleibend hohe Qualität der Dienstleistungen sicher. Zur Bewahrung und auch zum Nachweis der Qualität werden Accenture Delivery Center einer regelmäßigen Zertifizierung verschiedener Organisationen unterzogen. Diese Zertifizierungen bestätigen die kontinuierliche Einhaltung etablierter Best Practices und bieten ein hohes Maß an Sicherheit. Beispielsweise können hier CMMI, P-CMM, SAS70 oder ISO 27001 genannt werden.

7.2. Die zunehmende Bedeutung von Compliance für Outsourcing am Beispiel von British Telecom (BT)

British Telecom (BT) Group

Mit 18 Millionen Privat- und Geschäftskunden in 170 Ländern ist die BT Group ein weltweit führender Anbieter von Kommunikationsdienstleistungen und -lösungen. Das Angebot besteht aus IT-Services, lokalen, nationalen und internationalen Telekommunikationsdienstleistungen sowie Produkten und Dienstleistungen für Breitband und Internet.

Die Herausforderung

2006 startete die BT Group ein ehrgeiziges Programm zur Verbesserung der Finanzoperationen, welches unter anderem das Outsourcing von Finanztransaktionen beinhaltete. Als eines der Hauptziele wurde die Reduzierung von internen Kosten um bis zu 50 Prozent vorgegeben. Weitere Ziele waren unter anderem:

- Verbesserung des Kundenservice
- Standardisierung von Prozessen
- Verbesserung der operativen Effektivität und Transparenz
- Steigerung der Flexibilität
- **Verbesserung von Kontrollmaßnahmen und Compliance.**



Bereits einige Jahre zuvor hatte die BT Group zusammen mit Accenture Finance and Performance Management die Gestaltung eines neuen Geschäftsmodells für die Finanzfunktion erarbeitet. Aufbauend auf den positiven Erfahrungen aus bisherigen Projekten entschied sich die BT Group dafür, wieder mit Accenture zusammen zu arbeiten. Die langjährige Partnerschaft und Accentures praktische Erfahrungen sowie das umfassende Wissen im Bereich des Outsourcing von Finanztransaktionen waren entscheidende Gründe für die Entscheidung der BT Group.

Die Umsetzung

Auch die Umsetzung des Programms begann bereits im Jahr 2006, als nicht in Großbritannien getätigte Finanztransaktionen der BT Group in die Accenture Delivery Center Prag und Chennai (Indien) ausgelagert wurden. Mit dem zweiten Programmschritt im Jahr 2007 transferierte BT Group 50 Prozent aller Reporting-, Planung- und Analyse-Aktivitäten an Accenture. Mit diesem Schritt wurde BT Group zu einem Pionier auf dem Gebiet des Outsourcing von Finanzprozessen. Niemals zuvor hatte ein Großunternehmen entscheidungsunterstützende Finanzprozesse an einen Dritten ausgelagert.

Die Umsetzung dieses Programms umfasst zahlreiche Aktivitäten. Unter der Führung und Verantwortung von leitenden Managern der BT Group Finanzabteilung hilft Accenture bei:

- Bereitstellung von hochwertigen Finanz- und Buchhaltungsdienstleistungen, wie der Berichterstattung an das Management, Finanzplanung und -analyse, Monatsabschlüssen und Dienstleistungen zur Budgetierung und Kalkulation von Finanzkennzahlen aus dem Delivery Center in Chennai
- Entwicklung und Implementierung eines umfassenden, zuverlässigen Kontroll- und Compliance-Rahmenwerks, um die BT Group bei der Erreichung interner Leistungskennzahlen sowie der Erfüllung von Anforderungen des Sarbanes-Oxley Act zu unterstützen

- Automatisierung von strategisch weniger relevanten Reporting- und Analyse-Aktivitäten, wodurch Kapazitäten in der Finanzfunktion frei werden und zur Unterstützung der Analyse von Märkten, Industrien und Wettbewerbern eingesetzt werden können.

Die Ergebnisse

Seit dem ersten Programmschritt (dem Outsourcing von Finanztransaktionen) konnten die Transaktionskosten um 60 Prozent und die gesamten Betriebskosten im Finanzbereich um die Hälfte gesenkt werden. Die Realisierung dieser Leistungen hat die BT Group im Hinblick auf die allgemeinen Finanzkosten effizienter gemacht. Zusätzlich hat die umfassende Qualitätskontrolle einer großen Anzahl von Rechnungen dazu geführt, dass die damit verbundene Fehlerrate signifikant reduziert wurde; insbesondere zahlreiche Fehl- und Doppelzahlungen konnten vermieden werden.

Die erzielten Resultate spiegeln sich jedoch nicht nur in quantifizierbaren Werten wider. Die BT Group hat auch einen herausragenden Leistungsgrad in der Finanzfunktion erreicht und die unternehmensweite Transparenz von Aktivitäten, Ergebnissen und weiteren Anliegen der Finanzfunktion.

Transparenz und Messbarkeit gehen dabei Hand in Hand, weil die umfassende Auslagerung von Geschäftsprozessen eng mit einer umfassenden Messung von Leistungskennzahlen verknüpft ist. Finanzprozesse – und nicht nur deren einzelnen Aktivitäten – werden als Ganzes gemessen, analysiert und kommuniziert.

Die größere Flexibilität ist ein weiterer erreichter Erfolg, und nicht nur, weil die für die Strategie Verantwortlichen jetzt mehr Zeit für ihre eigentliche Aufgabe haben. Die BT Group verfolgt ehrgeizige Wachstumsziele – sowohl intern als auch durch Akquisitionen –, und diese können jetzt effektiv und ohne größere Störungen realisiert werden. Die ausgelagerten Finanzfunktionen – Mitarbeiter und Prozesse – sind jetzt in hohem Maße skalierbar. Das macht zukünftige Akquisitionen leichter, da zugekaufte Ressourcen in das Geschäftsmodell der BT Group eingefügt werden können.

Die Bedeutung und den Erfolg dieses Projektes belegt auch folgende Aussage von



Andrew Kemp, Direktor Reporting der BT Group, welcher in der Ausgabe April/Mai 2008 der Zeitung Financial and Administrative Outsourcing (FAO) Today sagte, dass „BT aufgrund dieses Projekts eine größere operative Leistungsfähigkeit, überdurchschnittlichen Kundenservice, standardisierte Prozesse, aussagekräftige Kennzahlen, eine größere Flexibilität, ein erhöhtes Maß an Transparenz und deutlich verbesserte Kontrollmaßnahmen sowie Compliance Aktivitäten erreicht habe“.

Dass Outsourcing mehr als nur der Fokus auf Kostenreduzierungen ist, zeigt abschließend folgende Aussage von Andrew Kemp: „BT decided on outsourcing as a key strategy because it gave us the ability to focus our attention on building a finance function that was able to add more value close to the customer, in terms of building decision support and value-added type activities...I think any organization that just does outsourcing for cost benefits is missing the big prize.“

7.3. Praxisorientierte Maßnahmen zur Beachtung von Compliance im Outsourcing

Wie bereits im ersten Teil dieser Studie erwähnt, verbleibt die Verantwortung für die ordnungsgemäße, sichere und gesetzeskonforme Abwicklung der ausgelagerten Aufgaben und Prozesse beim auslagernden Unternehmen bzw. dessen Geschäftsführung. Mit der zunehmenden Bedeutung von Compliance werden auch die Erwartungen an entsprechende Dienstleister bezüglich der professionellen Beachtung von Compliance in Outsourcing-Projekten noch weiter wachsen. Dies ergibt sich auch aus der Sorge vor einem Kontrollverlust und der möglichen Haftung für etwas, das nicht mehr im direkten Einflussbereich liegt. Neben wirtschaftlichen Gesichtspunkten und theoretischen Kenntnissen von Regularien rücken daher praktische Aspekte zur Minimierung von operativen Risiken in den Vordergrund.

Allerdings ist festzustellen, dass Compliance, obwohl es eines der prominentesten operativen Risiken ist, häufig noch nachrangig behandelt wird und entsprechende Anforderungen bereits in der Anbahnungs- bzw. Übergabephase nicht ausreichend berücksichtigt werden. Folgende typische Schwachstellen sind zu beobachten:

- Unsicherheit, welche Compliance-Regelungen in welchem Umfang umgesetzt werden müssen, bzw. ungenügende Abstimmung mit Kundenvertretern und Auditoren
- Unzureichende Zuordnung von Verantwortlichkeiten für die Umsetzung einzelner Compliance-Vorgaben
- Projektpläne und Arbeitspakete zur Umsetzung von Compliance sind nicht hinreichend definiert
- Fehlende Schulungen der funktionalen Teams bezüglich ihres Beitrags zur Umsetzung von Compliance im Outsourcing.

Um den künftig noch zunehmenden Herausforderungen von Compliance in Outsourcing-Projekten zu begegnen, sind diese Punkte bereits frühzeitig zu berücksichtigen und gemeinsam zu behandeln. Dies wird unterstützt durch die Etablierung eines zentralen Ansprechpartners auf Seiten des Outsourcing-Dienstleisters (Compliance Focal Point). Basierend auf den Angaben des auslagernden Unternehmens (und dessen Wirtschaftsprüfern) bemisst dieser den Umfang der umzusetzenden Regelungen, definiert und koordiniert entsprechende Arbeitspakete und Verantwortlichkeiten im Projekt und schult die funktionalen Projektteams entsprechend ihrer Aufgaben. Damit ist er zentrale Informationsstelle für alle das Outsourcing-Projekt betreffende Compliance-Themen.

Ebenso wie die Compliance-Thematik ganzheitlich koordiniert werden sollte, muss sie in den gesamten Auslagerungsprozess – von der Geschäftsanbahnung über tägliche Arbeitsabläufe bis hin zur Beendigung – verankert werden. Dabei gilt es, durch nachvollziehbare Maßnahmen das Risiko von Compliance-Abweichungen zu minimieren und dem Vertrauen, welches das auslagernde Unternehmen durch die Übergabe von Prozessen und Applikationen entgegen bringt, gerecht zu werden. Im Folgenden werden hierfür drei praxiserprobte Maßnahmen vorgestellt:

- Das Contract Management
- Die Operational Process Workbench
- Komplementäre Verfahren.



Das Contract Management

Um die Zusammenarbeit und damit die Rechte und Pflichten sowohl der Outsourcing-Kunden als auch der Outsourcing-Anbieter nachvollziehbar zu definieren und zu dokumentieren, werden im Rahmen von Auslagerungen komplexe Vertragswerke erstellt. Diese beinhalten unter anderem eindeutige Verantwortungs- und Leistungsbeschreibungen, Mess- und -Steuerungsprozesse sowie entsprechende Kennzahlen und sonstige rechtliche Rahmenbedingungen. Aufgrund der jeweiligen Situation der Outsourcing-Anbieter (beispielsweise durch Prozesslandschaften, Industriestandards oder sonstige Regularien) bedarf es umfangreicher und häufig auch langwieriger Verhandlungen, um die Auslagerung auch auf eine vertragliche Basis zu stellen. Hinzu kommt, dass Outsourcing-Verträge in der Regel mehrjährige Laufzeiten haben, die eine vertragliche Fixierung aller möglichen zukünftigen Änderungen unpraktikabel machen.

Der Einhaltung dieser vertraglich definierten Zusammenarbeit kommt somit eine Schlüsselrolle im Rahmen der Auslagerung zu. Um dieser Bedeutung gerecht zu werden, begleiten dedizierte Accenture-Vertragsfachleute („Contract Manager“) für alle relevanten Outsourcing-Projekte sowohl Vertragsgestaltung und -abschluss. Als Mitglieder des operativen Teams sind sie zuständig für die Einhaltung von Rechten und Pflichten aller Beteiligten während der eigentlichen Vertragslaufzeit. Damit wird während der gesamten Laufzeit – von der Verhandlungs- bis zur Beendigungsphase – die Vertragsgestaltung und -durchführung formalisiert und effizient überprüft. Bei Bedarf wird entsprechend im Rahmen von Change Requests oder Vertragsänderungen angepasst, operative und finanzielle Performance werden überwacht, was zu einer Reduzierung von Risiken und zur Weiterentwicklung einer vertrauensvollen Geschäftsbeziehung beiträgt. Der Contract Manager umfasst dabei die folgenden 3 Rollen und Verantwortlichkeiten:

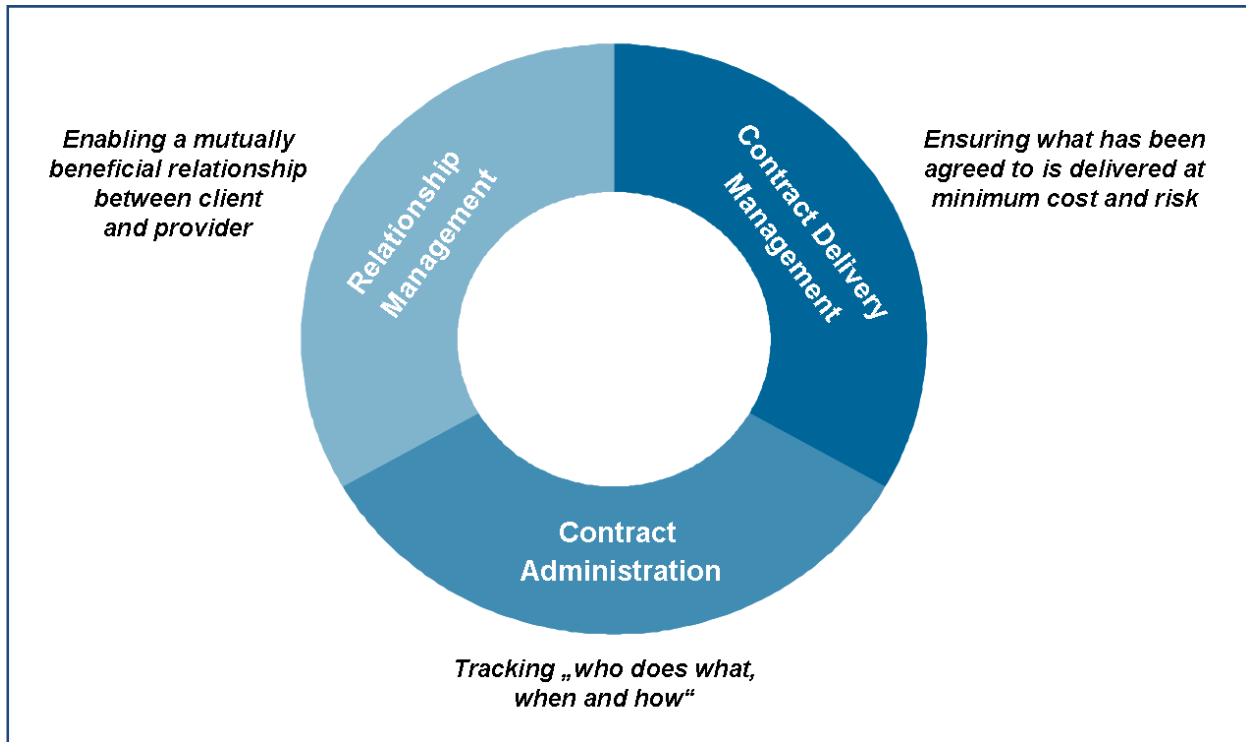


Abbildung 9: Rollen und Verantwortlichkeiten des Contract Manager (eigene Darstellung).

Accenture Contract Manager begleiten relevante Outsourcing-Projekte sowohl zur Einhaltung vertraglicher Rechte und Pflichten als auch zur pro-aktiven Veranlassung von Verbesserungsmaßnahmen. Dies trägt signifikant zu einer erfolgreichen Durchführung von Auslagerungsaktivitäten bei – sowohl für den Outsourcing-Kunden als auch den -Dienstleister.

Die Operational Process Workbench

Bei einer Entscheidung für Outsourcing verändern sich Arbeitsabläufe und Prozesse grundlegend und unabhängig von den Gründen, die zu dieser Entscheidung führen – sowohl bei den Outsourcing-Kunden als auch bei den beteiligten Dienstleistern. Meist langjährig etablierte und teilweise definierte Prozesse müssen angepasst, zu meist aber völlig neu definiert und implementiert werden. Dies stellt Outsourcing-Kunden und -Dienstleister immer wieder vor große und meist auch kostenintensive Herausforderungen, die bereits zum Projektstart einkalkuliert werden müssen.

Um diesen Herausforderungen effizient und koordiniert zu begegnen, vereint Accenture langjährige Praxiserfahrungen in den folgenden sieben Bereichen zu einer Disziplin: der Operational Excellence. Operational Excellence, Accentures Ansatz zur Sicherstellung von Effektivität und Effizienz in den täglichen Arbeitsabläufen, beruht auf einer Standardisierung der Prozesse und deren Messbarmachung sowie der strikten Befolgung bewährter Methoden und Verfahren. Operational Excellence wird bei allen Accenture Outsourcing-Projekten verpflichtend angewendet.



Abbildung 10: Operational Excellence (eigene Darstellung).

Operational Excellence wird dabei durch verschiedene harmonisierte Hilfsmittel unterstützt. Beispielsweise steht mit der Operational Process Workbench (OPW) ein Prozessmanagement- und Prozessdokumentations-Tool zur Verfügung, das die Durchführung leistungsfähiger und stabiler Prozesse ermöglicht. Dieses liefert den Outsourcing-Kunden kontrollierbare, messbare, wiederholbare und berechenbare Dienstleistungen. Die Methoden der OPW werden dabei über den gesamten Outsourcing-Lebenszyklus hinweg angewandt, d.h. schon vom Beginn der Übergangsphase (unter Koordination des Compliance Focal Points). Die OPW ist aber weit mehr als ein Dokumentations-Werkzeug. Vielmehr werden auf einer gemeinsamen

Plattform das Design und die Freigabe, die Archivierung sowie die kontrollierte Änderung von Prozessen konsistent umgesetzt. Dabei werden alle Prozesse, Dokumentationen und prozessbegleitenden Informationen (z.B. Arbeitsschritte oder Rollen) miteinander verknüpft und zentral vorgehalten. Beispielhafte Eigenschaften des OPW sind:

- Prozesse, inkl. graphischer Darstellungen und Dokumentationen, werden für alle Anwender sichtbar
- Prozesse werden mit Rollen, Systemen, Kontrollen, Ergebnissen von Kontrollaudits sowie Arbeitsanweisungen verknüpft und somit Interdependenzen sichtbar gemacht
- Die Identifizierung und Steuerung von Prozessrisiken wird ermöglicht.

Der Zugriff auf das OPW kann von multiplen Anwendern, verteilt auf verschiedenste geographische Regionen, erfolgen („one host – multiple clients“).

Um das operative Risiko von Compliance-Verstößen zu minimieren, müssen alle Aktivitäten nachvollziehbar anhand eines übergeordneten Verfahrens ausgerichtet sein. Gerade im Bezug auf Compliance ist Operational Excellence, unterstützt durch die richtigen Hilfsmittel, ein elementarer Bestandteil des täglichen Handelns.

Komplementäre Verfahren

Zusätzlich zu den anerkannten, nachvollziehbaren Arbeitsabläufen werden von Accenture im Rahmen von Outsourcing-Projekten auch komplementäre Verfahren zur Sicherstellung der Ordnungsmäßigkeit von Prozessinformationen angeboten. Diese Verfahren gehen über Standarddienstleistungen hinaus und etablieren sowohl wirksame als auch wirtschaftliche Überwachungsmaßnahmen durch die intelligente Nutzung von Informationstechnologie.

Im Folgenden werden zwei Verfahren sowohl zur „ad-hoc“ als auch zur kontinuierlichen Überwachung von Geschäftsprozessen finanzieller Art und deren Transaktionen vorgestellt: das Accenture Transaction Compliance & Analytics Tool (ATCAT) sowie Continuous Controls Monitoring (CCM).



- Das Accenture Transaction Compliance & Analytics Tool (ATCAT) wurde speziell dazu entwickelt, Fehler wie Doppelzahlungen zu vermeiden. Dies wird vor allem durch die Verwendung von hoch entwickelten Suchalgorithmen realisiert, welche hierfür besser geeignet sind als die Standardlösungen in ERP-Systemen. Dies ist ein entscheidender Wandel im Finanz- und Buchhaltungsmanagement und eine bedeutsame Chance für Unternehmen. ATCAT ermöglicht einen Wechsel von einer zyklischen, rein zahlungsnachgelagerten Prüfung hin zu einem vorbeugenden Kontrollumfeld, das Fehler identifiziert, bevor sie geschehen (detektivisch). Somit kann eingegriffen werden, bevor eine Zahlung erfolgt. Wird ein Fehler wie eine Mehrfachzahlung entdeckt, sendet das System automatisch eine entsprechende Benachrichtigung an einen vorher festgelegten Empfänger, der weitere Schritte wie eine Ursachenanalyse einleiten kann. Durch die tief greifende Analyse der Zahlungsvorgänge können außerdem Verbesserungen im Purchase-to-Pay-Prozess identifiziert und realisiert werden. ATCAT ist dabei ein flexibles Tool, das so aufgesetzt ist, dass es einfach und schnell in jedes ERP- oder Supply Chain Management-Umfeld integriert werden kann.
- Einen Schritt weiter geht der Ansatz von Continuous Controls Monitoring (CCM). CCM ist die kontinuierliche Anwendung von Kontrollen auf prozessabhängige Transaktionsdaten (beispielsweise aus dem Beschaffungsprozess oder Zeit-/Spesenabrechnungen). Dabei definiert das auslagernde Unternehmen gemäß seiner aktuellen Risikosituation Kontrollaktivitäten (z.B. Kontrollen zur Funktionstrennung, Belegintegrität oder Zahlungsüberwachungen), welche anschließend automatisiert auf die im Tagesablauf generierten Geschäftstransaktionen angewendet werden. Durch die kontinuierliche (in der Regel tägliche) Anwendung von automatisierten Kontrollen können fehlerhafte Abläufe oder sogar unrechtmäßige Handlungen zeitnah aufgedeckt werden. Durch diesen höheren Abdeckungsgrad als bei manuellen, stichprobenartigen und zeitlich eingeschränkten periodischen Kontrollen erhöht CCM signifikant die Transparenz der Geschäftsprozesse und steigert die Einsicht in Prozessineffizienzen und -risiken. Somit können dem auslagernden Unternehmen zu-

sätzliche, in der Regel sogar monetär messbare Informationen zur Verfügung gestellt werden, um der bei ihm verbleibenden Verantwortung eindeutig gerecht zu werden.

Die vorgestellten Verfahren tragen in erster Linie zur weiteren Sicherstellung ordnungsgemäßer Abläufe bei und gehen über das bloße Erreichen von Compliance im Outsourcing hinaus. Durch die kontinuierliche und automatisierte Anwendung von Kontrollen auf Massenbeständen an Daten werden zusätzlich Informationen über die Effizienz und Risikobeschaffenheit von Prozessen auf intelligente Weise gewonnen (Compliance Intelligence). Mit diesem Ansatz wird über die Pflichterfüllung hinaus der Weg zu mehr Effizienz, besserem Risikomanagement und höherer Wertschöpfung im Outsourcing gewiesen.



8. Fazit

Ziel der vorliegenden Studie war die Identifikation der theoretischen Grundlagen und praktischen Anforderungen im Bereich Compliance, die derzeit beim IT-Outsourcing zu beachten sind. Zudem sollte untersucht werden, wie Unternehmen gegenwärtig auf Compliance-Anforderungen reagieren und welche Best Practices bestehen.

Die theoretische Grundlage der Studie basiert auf einer Bestimmung der Begriffe Compliance (bzw. IT-Compliance) und IT-Outsourcing. Ausgehend von der inzwischen untrennbaren Verzahnung von betrieblichem Handeln und Informationstechnologie wurde Compliance als eine in Zusammenhang mit Governance und Risikomanagement zu sehende Aufgabe der Unternehmensführung (bzw. des IT-Managements) definiert. Daran schloss sich eine sowohl theoretische als auch praktische Bestimmung des IT-Outsourcing und seiner Formen an, die auch eine kritische Betrachtung wichtiger Argumente für oder gegen Outsourcing-Entscheidungen beinhaltet (Argumentenbilanz des IT-Outsourcing).

Die Anforderungen aus Compliance-Sicht, die beim IT-Outsourcing beachtet werden müssen, lassen sich in gesetzliche Regelungen wie SOX und die 8. EU Richtlinie, in Richtlinien, Standards und Referenzmodelle (oder Rahmenwerke wie COSO, COBIT und CCMI) sowie in innerbetriebliche Bestimmungen unterteilen. Angesichts der Dynamik der Entwicklung im Bereich Compliance lassen sich diese noch nicht abschließend beurteilen; das gilt insbesondere für die Standards und Referenzmodelle. Dabei erweist sich die Zertifizierung von internationalen Standards und Referenzmodellen gerade für Outsourcing-Anbieter zunehmend als Wettbewerbsvorteil. Schon heute erscheint es für Outsourcing-Anbieter sinnvoll, Compliance anhand von SAS 70 zu bescheinigen. Es ist also zu erwarten, dass Zertifizierungen zu einem immer wichtigeren Kriterium bei der Auswahl von Outsourcing-Anbietern werden und diese in Zukunft noch mehr bestrebt sind, für qualitativ hochwertige Verfahren Zertifizierungen zu erhalten. Dies wird auch dem steigenden Druck der Outsourcing-Kunden folgen, formalisierte Abläufe zur Steigerung der Prozesseffektivität und -effizienz objektiv zu belegen.

Eine Analyse von Compliance-spezifischen Anforderungen mit Bezug auf IT-Outsourcing ergab, dass es für Outsourcing-Kunden und -Anbieter sowohl Pro- als auch Contra-Argumente gibt. Kostenersparnisse, Effizienzsteigerungen, die Erhöhung von Prozesstransparenz und das Aufzeigen von Verbesserungspotentialen sprechen für die Zusammenarbeit mit spezialisierten Anbietern. Dies ist insbesondere vor dem Hintergrund einer wirksamen und wirtschaftlichen Governance für Geschäftsprozesse und Unternehmens-IT bedeutsam. Verursacht durch immer komplexer werdende regulatorische Vorgaben können Outsourcing-Anbieter wiederum mit einer verstärkten Nachfrage rechnen. Dieser können sie nicht nur durch Preis- sondern auch durch Qualitätsargumente begegnen.

Die aufgeführten Argumente gegen das IT-Outsourcing, begründet durch Compliance-Anforderungen, verdichten sich im Wesentlichen zum Argument der massiven Komplexitätssteigerung für beide Outsourcing-Parteien. Für Outsourcing-Kunden ergeben sich durch die Auslagerung deutliche Komplexitätssteigerungen um sicherzustellen, dass die einzuhaltenden Vorschriften auch durch die Outsourcing-Anbieter befolgt werden. Für Outsourcing-Anbieter entstehen in erster Linie Nachteile durch Zusatzaufgaben, die preissensitiv umgesetzt werden müssen. Zusätzlich erhöht sich die Komplexität in der täglichen Arbeit, was sich auch in umfangreicher werdenden Vertragsstrukturen widerspiegelt.

Nicht zuletzt aus diesen Gründen ist Compliance ein eminent wichtiger Faktor in der Entscheidungsfindung. Anders als in der Literatur wird IT-Outsourcing unter Compliance-Aspekten in der Praxis jedoch bereits stark beachtet. Die quantitativ-explorativen Expertenbefragung lieferte mit einer Teilnahme von 132 Experten ein aussagekräftiges Meinungsbild der Praxis und unterstreicht mit einer Rücklaufquote von 56% die Aktualität dieser Thematik. Die Studie zeigte, dass Compliance-Aspekte bei der Entscheidungsfindung für oder gegen IT-Outsourcing eine wichtige Rolle spielen. Dies hat insbesondere einen Grund: Die Verantwortung für Compliance kann durch IT-Outsourcing nicht übertragen werden, und Unternehmen stehen auch dann in der rechtlichen Verantwortung für „ihre“ IT-Systeme und Prozesse, wenn diese vollständig an einen Outsourcing-Dienstleister ausgelagert werden. Daher überrascht es auch nicht, dass Rahmenwerke, Zertifikate und Standards sich als wichtiges Mittel



zum Nachweis von Compliance in IT-Outsourcing-Beziehungen etabliert haben (insbesondere der SAS 70-Report).

Als Ergebnis der Umfrage bleibt festzuhalten, dass Compliance-Aspekte als Argument für bzw. gegen das IT-Outsourcing eine eminent wichtige Rolle spielen. Daher sollte Compliance als eigenständiges Kriterium in die Entscheidungsmodelle zum IT-Outsourcing aufgenommen werden. Allerdings finden sich hierzu keine formalisierten Entscheidungsmodelle. Zudem ist es für die Zukunft unerlässlich, den aktuellen Compliance-Ansatz zu einem strategischen Instrument der Unternehmensführung auszubauen. Hierzu müssen Governance, Risikomanagement und Compliance in ein Managementkonzept integriert und gemeinsam weiterentwickelt werden; ebenso wenig wie Governance-Vorgaben und das Risikomanagement darf sich die Erfüllung von Compliance nicht auf reaktive, isolierte Maßnahmen beschränken. Daher ist es wichtig, dass die Umsetzung von Compliance bei Auslagerungsvorhaben pro-aktiv und konsequent vorgenommen wird.

Compliance im IT-Outsourcing ist nicht nur eine nicht verhandelbare Pflicht, sondern kann für beide Outsourcing-Parteien einen messbaren Mehrwert bieten.

VII. Literaturverzeichnis

- [Accenture 2008]** Accenture: The Changing Role of the Finance Organization in a Multi-Polar World: Accenture High Performance Finance Study 2008.
URL: http://www.accenture.com/Global/Research_and_Insights/By_Subject/Finance_Mgmt/Finance_Operations/TheChangRole2008.htm
- [Amberg et al. 2006]** Amberg, M.; Wiener, M.: IT-Offshoring. Management internationaler IT-Offshoring-Projekte. Physica, Heidelberg 2006.
- [Amberg et al. 2007]** Amberg, M.; Mossanen, K.: Vorteile und Herausforderungen IT-gestützter Compliance Erfüllung. URL: http://www.wi3.uni-erlangen.de/fileadmin/Dateien/Publikationen/Executive_Summary_IT-Compliance.pdf
- [Annuscheit 2006]** Annuscheit, R.: Erfüllung von Compliance-Aufgaben. In: Compliance-Magazin (Hrsg.)-online-Fachbeiträge-Management, 2006.
URL: <http://www.compliance-magazin.de/compliancefachbeitraege/management/ca271106.html>
- [Behrens 2007]** Behrens, S.: Information systems outsourcing. Five essays on governance and success. In: Research in information systems, Bd. 4. Dissertation der European Business School Wiesbaden, Shaker, Aachen 2007.
- [BITKOM 2006]** BITKOM (Hrsg.): Compliance in IT-Outsourcing- Projekten. Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen. Berlin 2006.
URL: http://www.bitkom.org/de/themen_gremien/36129_40787.aspx
- [CGI 2005]** CGI Group inc (Hrsg.): IT Governance and Managed Services, in: CGI-online – Know-how – White Papers, 2005.
URL: http://www.cgi.com/cgi/pdf/cgi_whpr_59_gov_manag_serv_e.pdf
- [CIO 2007]** CIO Online (Hrsg.): Deutscher IT-Outsourcing-Markt wächst deutlich. In: Knowledge Center – Outsourcing, 2007.
URL: <http://www.cio.de/knowledgecenter/outsourcing/840909/>
- [DCGK 2008]** Regierungskommission Deutscher Corporate Governance Kodex – in der Fassung vom 6. Juni 2008, Ziffer 4.1.3.
URL: http://www.corporate-governance-code.de/ger/download/D_Kodex%202008_final.pdf
- [Fröhlich et al. 2007a]** Fröhlich, M.; Glasner, K. : IT Governance - Leitfaden für eine praxismgerechte Implementierung, Wiesbaden 2007.
- [Gaulke 2006]** Gaulke, M.: COBIT als IT-Governance-Leitfaden, in: Fröschle, H. -P.; Strahinger, S. (Hrsg.): IT-Governance. HMD - Praxis der Wirtschaftsinformatik, Heft 250, 2006, S. 21-28.
- [GDPdU 2001]** Bundesministerium für Finanzen (Hrsg.): Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), in: Schreiben des BMF vom 16. Juli, 2001.
URL: http://www.bundesfinanzministerium.de/nn_314/DE/BMF_Startseite/Aktuelles/BMF_Schreiben/Veroeffentlichungen_zu_Steuerarten/abgabenordnung/006.templateId=ra_w.property=publicationFile.pdf



- [GoBS 1995]** Bundesministerium für Finanzen (HrsG.): Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), in: Schreiben des BMF vom 7. November, 1995. URL: <http://www.elektronische-steuerpruefung.de/rechtsgrund/gobs.pdf>
- [Goeken et al. 2006]** Goeken, M.; Johannsen, W.: IT-Governance – neue Aufgaben des IT-Managements, in: Fröschle, H. -P.; Strahinger, S. (Hrsg.): IT-Governance. HMD - Praxis der Wirtschaftsinformatik, Heft 250, 2006, S. 7-20.
- [Hall et al. 2007]** Hall, J.; Liedtka, S.: The Sarbanes-Oxley Act: Implications for Large Scale IT-Outsourcing, in: Communications of the ACM, Vol. 50, No. 3, 2007.
- [Heinze et al. 2005]** Heinze, T.; Menzies, C.: Die Rolle der IT bei der Umsetzung des Sarbanes-Oxley Act, in: Sicherheit & Datenschutz, Ausg. 8, 2005, S. 78-85.
- [Hermes et al. 2005]** Hermes, H.-J.; Schwarz, G. (Hrsg.): Outsourcing. Chancen und Risiken, Erfolgsfaktoren, rechtssichere Umsetzung. Haufe, Freiburg u.a. 2005.
- [Hirschheim et al. 2004]** Hirschheim, R.; George, B.; Wong, S. F. (2004): Information technology outsourcing: The move towards offshoring. In: Indian Journal of Economics & Business, Special Issue, 2004, pp. 103-123.
- [Huissoud 2001]** Huissoud, M.: IT-Outsourcing und Revision - Konsequenzen des IT Outsourcings für die interne und externe Revision, in: Eidgenössische Finanzkontrolle-online – Fachtexte, 2001. S. 182-185. URL: http://www.efk.admin.ch/pdf/it-outsourcing%20und%20revision_d.pdf
- [Kampffmeyer 2006]** Kampffmeyer, U.: Compliance: Rechtliche Anforderungen an die elektronische Dokumentation, in: Project Consult-online – Download, 2006. URL: http://www.project-consult.net/Files/Ingram_Compliance.pdf
- [Kersten 2008]** Kersten, H.; Reuter, J.; Schröder, K.-W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Wiesbaden 2008.
- [Klotz 2007]** Klotz, M.: IT-Compliance - auf den Kern reduziert, in: IT-Governance. Zeitschrift des ISACA Germany Chapter e. V., Heft 1, 2007, S. 14-18.
- [Knolmayer et al. 1998]**
Knolmayer, G.; Mertens, P.: Organisation der Informationsverarbeitung. Grundlagen-Aufbau-Arbeitsteilung. 3. Aufl., Gabler, Wiesbaden 1998.
- [Knolmayer 2007]** Knolmayer, G.: Compliance Nachweise bei Outsourcing von IT-Aufgaben, in: Wirtschaftsinformatik, Heft 49 (Sonderheft), 2007, S. 98-106.
- [Krcmar 2005]** Krcmar, H.: Informationsmanagement. 4. Aufl., Springer, Berlin u.a. 2005.
- [Lanfermann 2005]** Lanfermann, G.: Modernisierte EU-Richtlinie zur gesetzlichen Abschlussprüfung. In: Der Betrieb, Heft 49, 2005, S. 2645-2650.
- [Lui 2005]** Lui, B.: Implikationen des operationellen Risikos nach Basel II für die Informationstechnologie. In: Becker, A.; Gaulke, M; Wolf, M. (Hrsg.): Praktiker Handbuch

Basel II. Kreditrisiko, Operationelles Risiko, Überwachung, Offenlegung. Schäffer-Poeschel, Stuttgart 2005.

[Nörr et al. 2005] Nörr, Steifenhofer, Lutz (Hrsg.): Chefsache IT-Sicherheit, Abschlussprüfung,- Basel II,- SOX,- Vorstandshaftung,- KonTraG,- UMAG, In: Broschüren & Newsletter, 2005.

URL: http://www.noerr.com/PortalData/1/Resources/90_metanavigation/broschueren_und_newsletter/spezielle_themen/NSL_brosch%C3%BCre_IT-sicherheit_051207.pdf

[Orange 2007] Orange (Hrsg.): CxO survey 2007 – results. Outsourcing Services. In: Orange, Knowledge Center, 2007.

URL: http://www.mnc.orange-business.com/content/pdf/OBS/library/business_briefs/bizbrief_outsourcing_cxo_survey.pdf

[Pallast 2002] Pallast, L. R.: Vorteile des Application Management gegenüber anderen Outsourcing Modellen. In: Köhler-Frost, W. (Hrsg.): Allianzen und Partnerschaften im IT-Outsourcing. KSE, Berlin 2002, S. 162-181.

[Perdata 2008] Perdata (Hrsg.): Umfassende IT-Sicherheit bestätigt: perdata absolviert erfolgreich Zertifizierung nach ISO 27001. Pressemitteilung. In: Perdata-online – Presse, 2008.

URL: <http://www.perdata.de/presse>

[Steria Mummert 2007] Steria Mummert Consulting (Hrsg.): Kreditwirtschaft: Gesetzliche Vorgaben treiben Risikomanagement voran. In: Steria Mummert-online – Pressearchiv, 2007.

URL: <http://www.steria-mummert.de/presse/pressearchiv/1.-quartal-2007/kreditwirtschaft-gesetzliche-vorgaben-treiben-risikomanagement-voran>

[Yang 2000] Yang, C.; Huang, J. B.: A decision model for IS outsourcing. In: International Journal of Information Management, Vol. 20, 2000, pp. 225-239.

VIII. Autoreninformationen

Prof. Dr. Michael Amberg, geboren 1961, ist Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik III, an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Seit April 2007 ist Prof. Amberg Dekan der Wirtschafts- und Sozialwissenschaftlichen Fakultät und wurde im Oktober 2007 für weitere 3 Jahre in seinem Amt als Dekan der neu strukturierten Gesamtfakultät Rechts- und Wirtschaftswissenschaften der FAU Erlangen-Nürnberg bestätigt. Zuvor war er an der Universität Bamberg und an der RWTH in Aachen tätig.



Die Forschungsschwerpunkte des Lehrstuhls liegen insbesondere auf den „weichen“ Faktoren der Entwicklung und des Einsatzes von Informationstechnologien. Hierzu zählen derzeit IT-Projektmanagement, IT-Offshoring/ Outsourcing, Kompetenzmanagement, Enterprise Architecture, Compliance Management, Requirements Management und die strategischen Auswirkung von service-orientierten Unternehmens-Architekturen.

Herr Dipl.-Kfm. **Kian Mossanen** hat 2006 das Studium der Betriebswirtschaftslehre an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) als Diplom-Kaufmann abgeschlossen. Dabei absolvierte er Studienaufenthalte in Mexico und den USA. Seither ist er wissenschaftlicher Mitarbeiter am Lehrstuhl für Betriebswirtschaftslehre, insbes. Wirtschaftsinformatik III, an der FAU. Außerdem ist er als Assistent der Geschäftsleitung eines deutschen Konzerns im Bereich IT-Solutions and Services tätig.



Im Rahmen seiner Dissertation beschäftigt sich Herr Mossanen mit dem Thema Compliance und untersucht dabei im Speziellen Aspekte der Wirtschaftlichkeit sowie Auswirkungen von Compliance auf das IT-Outsourcing.

Herr Dipl.-Volkswirt **Winfried Kramolisch** hat 2008 das Studium der Volkswirtschaftslehre an der Friedrich-Alexander-Universität Erlangen-Nürnberg als Diplom-Volkswirt abgeschlossen. Dabei sammelte er Berufserfahrungen bei Infineon Technologies North America und Air France/KLM in der russischen Föderation. Außerdem nahm er im Rahmen eines Studienaufenthaltes am Master of International Business Program der State University, School of Management St. Petersburg teil. Bis Dezember 2008 war Herr Kramolisch im International Financial Management der Siemens AG im Bereich IT-Solutions and Services tätig. Seit Dezember 2008 ist er Assistent der kaufmännischen Geschäftsleitung im Bereich IT-Solutions and Services.



Herr **Sven Biermann** studierte Finanz-, Prüfungs- und Steuerwesen sowie Informationsmanagement in Deutschland und den USA mit Abschlüssen als Diplom-Betriebswirt (FH) und Master of Business Administration.

Herr Biermann ist seit 2001 als Berater für die Accenture GmbH im Bereich Finance & Performance Management in München tätig. Er leitet dort die Gruppe zur unternehmensweiten Implementierung von Compliance Intelligence. Er hat zahlreiche Publikationen im Bereich Compliance veröffentlicht und ist aktives Mitglied in diversen internationalen Gremien (u. a. dem United Nations Global Compact).



Herr **Dr. Leo Lehr** studierte Physik und Betriebswirtschaftslehre in Deutschland und Amerika mit Abschlüssen in Physik und Diplom-Wirtschaftsphysik. Darüber hinaus promovierte er im Bereich Biophysik an der Universität München.

Seit 2001 ist Herr Dr. Leo Lehr als Berater für die Accenture GmbH tätig. Seine Schwerpunkte liegen in den Bereichen Corporate Finance & Accounting sowie Finance and Performance Management. Als anerkannter Experte hat er zahlreiche große Design- und Implementierungsprojekte mit Offshore-Anteilen in Indien und den Philippinen unter anderem auch in den Themenbereichen Compliance und Continuous Controls Monitoring geleitet. Herr Dr. Lehr ist an zahlreichen Büchern und Fachbeiträgen zu aktuellen Themen und Fragestellungen im Finanzbereich beteiligt





IX. Accenture

Accenture ist ein weltweit agierender Managementberatungs-, Technologie- und Outsourcing-Dienstleister. Das Unternehmen bringt umfassende Projekterfahrung, fundierte Fähigkeiten über alle Branchen und Unternehmensbereiche hinweg und Wissen aus qualifizierten Analysen der weltweit erfolgreichsten Unternehmen in eine partnerschaftliche Zusammenarbeit ein. So schafft Accenture für seine Kunden nachhaltigen Markterfolg. Das Unternehmen beschäftigt rund 186.000 Mitarbeiter in 49 Ländern und erwirtschaftete im vergangenen Fiskaljahr (zum 31. August 2008) einen Nettoumsatz von 23,39 Mrd. US-Dollar. Die Internetadresse lautet www.accenture.de.