

■ Impressum

Herausgeber:

BITKOM

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Albrechtstraße 10

10117 Berlin-Mitte

Telefon 030/27576-0

Telefax 030/27576-400

bitkom@bitkom.org

www.bitkom.org

Redaktion: Dr. Mathias Weber

Verantwortliches BITKOM-Gremium:

Projektgruppe „Compliance in IT-Outsourcing-Projekten“ im Arbeitskreis Outsourcing

Redaktionsassistentin: Anna Rosenberger, BITKOM

Stand: Juli 2006

Die Inhalte dieses Leitfadens sind sorgfältig recherchiert. Sie spiegeln die Auffassung im BITKOM zum Zeitpunkt der Veröffentlichung wider. Die vorliegende Publikation erhebt jedoch keinen Anspruch auf Vollständigkeit. Wir übernehmen trotz größtmöglicher Sorgfalt keine Haftung für den Inhalt.

Der jeweils aktuelle Leitfaden kann unter www.bitkom.org/publikationen kostenlos bezogen werden. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim BITKOM.

Der Leitfaden „Compliance in IT-Outsourcing-Projekten“ erweitert das Spektrum der BITKOM-Publikationen zum Outsourcing:

- „BITKOM-Positionierung zum Thema ITO“
- „ITO Terminologie“
- „Offshore-Leitfaden“
- „IT-Outsourcing im Öffentlichen Dienst“
- „Leitfaden Ausrichtung der IT bei Business Process Outsourcing“
- „Business Process Outsourcing – Leitfaden. BPO als Chance für den Standort Deutschland“
- „Offshore-Report 2005“

Ansprechpartner:

Dr. Mathias Weber, BITKOM e.V.

Tel: 030/27576-121

E-Mail: m.weber@bitkom.org

Geleitwort

Zahlreiche gesetzliche Vorschriften und zunehmender Druck von Finanzmärkten stellen Führungskräfte aus der Wirtschaft vor neue Herausforderungen, denn die IT-Systeme und Geschäftsprozesse in den Unternehmen müssen den komplexen gesetzlichen Auflagen entsprechen. Neue Anforderungen an Corporate Governance und Compliance machen auch um Outsourcing-Dienstleistungen keinen Bogen. Folgende Fragen sind für Kunden und Anbieter von Outsourcing-Services gleichermaßen aktuell:

- Welche gesetzlichen Regelungen und Richtlinien sind bei IT-Outsourcing-Projekten zu beachten?
- Welche Standards oder Zertifikate haben sich auf dem Markt durchgesetzt?
- Welche Referenzmodelle bieten Orientierungen?
- Wie sollten sich die neuen Anforderungen in einem Outsourcing-Vertrag widerspiegeln?
- Wie setze ich als Verantwortlicher im Unternehmen diese Richtlinien praktisch um?



Prof. h.c. Jörg Menno Harms
Vizepräsident BITKOM

Einschlägige Standards sowie rechtliche Rahmenbedingungen und deren vertragliche Umsetzung werden bei der Planung und Umsetzung von Outsourcing-Projekten nur allzu leicht übersehen.

Die eher juristische Ausrichtung der genannten Fragestellungen mag manchen Leser zurückschrecken lassen. Der Leitfaden soll Entscheidungsträger auf die Relevanz der hier aufgeworfenen Fragestellungen aufmerksam machen und ihnen den notwendigen Überblick verschaffen. Er bietet eine komprimierte Zusammenstellung der relevanten Gesetze, Richtlinien, Standards sowie Ansätze und Hilfestellung zur praktischen Umsetzung.

Die Publikation zeigt: Compliance in IT-Outsourcing-Projekten ist beherrschbar!

A handwritten signature in black ink, appearing to read 'J. Menno Harms'.

Prof. h. c. Jörg Menno Harms
Vizepräsident des BITKOM

Projektteam

Dank der wertvollen Unterstützung der Arbeitskreismitglieder und deren konstruktiver und kontinuierlicher Mitarbeit konnte dieser Leitfaden entstehen. Besonderer Dank gilt dabei den Autoren und der Redaktion.

- Wolfgang Ebert, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, München, E-Mail: wolfgang.ebert@de.pwc.com
- Christina Hübschen, Accenture, Kronberg/Ts., E-Mail: christina.huebschen@accenture.com
- Robert Jung, Accenture, Düsseldorf, E-Mail: robert.jung@accenture.com
- Dr. Lars Lensdorf, Heymann & Partner Rechtsanwälte, Frankfurt am Main, E-Mail: L.Lensdorf@heylaw.de
- Dr. Jan Geert Meents, CMS Hasche Sigle Rechtsanwälte Steuerberater, München, E-Mail: jan.meents@cms-hs.com
- Roman Mohry, IBM Deutschland GmbH, Düsseldorf, E-Mail: mohry@de.ibm.com
- Wolfgang Patschke, Satyam Computer Services Ltd., Wiesbaden (Nordenstadt), E-Mail: wolfgang_patschke@satyam.com
- Dr. Stephan Scholtissek, Accenture, München, E-Mail: stephan.scholtissek@accenture.com (Sprecher des Projektteams)
- Ulrich Schroth, Deloitte & Touche GmbH, Frankfurt am Main, E-Mail: uschroth@deloitte.de
- Dr. Peter Spitzner, 3wBox GmbH, Nürnberg, E-Mail: peter.spitzner@3wbox.de
- Dr. Mathias Weber, BITKOM e.V., E-Mail: m.weber@bitkom.org
- Heino Wehran, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Hannover, E-Mail: heino.wehran@de.pwc.com
- Stefan Weiss, Deloitte & Touche GmbH, Frankfurt am Main, E-Mail: stefanweiss@deloitte.de
- Dr. Andrea Wiehler, Info AG Gesellschaft für Informationssysteme, Hamburg, E-Mail: andrea.wiehler@info-ag.de

Inhalts- Abbildungs- und Tabellenverzeichnis

1	Executive Summary	11
2	Compliance, Reifegrad einer IT-Organisation und Outsourcing	13
2.1	Bedeutung von Compliance in Outsourcing-Entscheidungen	13
2.2	Wertschöpfung der IT und ihrer auszulagernden Teile.....	15
2.3	Das Risiko auslagern?	16
3	Vorschriften und Standards im Outsourcing.....	18
3.1	Einführung	18
3.2	Relevanz für IT-Outsourcing.....	22
3.3	Kurze Darstellung der einschlägigen gesetzlichen Regelungen.....	25
3.3.1	Auswahlkriterien	25
3.3.2	Gesetz zur Kontrolle und Transparenz - Haftungsregelung	25
3.3.3	GmbH Gesetz – Sorgfaltspflicht und Ordnungsmäßigkeit	26
3.3.4	Handelsgesetzbuch – Überprüfung ausgelagerter Buchführung	26
3.3.5	Bundesdatenschutzgesetz - Verarbeitung personenbezogener Daten	27
3.3.6	Sarbanes-Oxley-Act – Vorschriften für Kontrollsysteme	28
3.4	Richtlinien, Grundsätze und Rundschreiben.....	29
3.4.1	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen	29
3.4.2	Baseler Eigenkapitalvereinbarung.....	29
3.4.3	Rundschreiben und sonstige Bekanntmachungen der BaFin.....	30
3.5	Normen und Standards	31
3.5.1	Buchführungs-Standards	31
3.5.2	Wirtschaftsprüfungs-Standards.....	32
3.5.3	Prüfungs- oder Implementierungs-Standards für die Zertifizierung von IT-Prozessen.....	33
3.5.4	DIN-, ISO-, IEC-Normen und Best Practice.....	37
3.6	Referenzmodelle.....	38
4	Risiken der Nichteinhaltung und vertragliche Abbildung rechtlicher Rahmenbedingungen	41
4.1	Überblick.....	41
4.2	Sanktionen und Haftungsrisiken	42
4.2.1	Allgemeines	42
4.2.2	Spezielle Verantwortung der Geschäftsleitung.....	43
4.2.3	Aufsichtsrat.....	44
4.2.4	Absicherung durch Directors & Officers Versicherung	44
4.3	Aspekte der Vertragsgestaltung	45
4.3.1	Schaffung einer Basis für eine langfristige Beziehung.....	45
4.3.2	Klare Definition und Abgrenzung der Verantwortlichkeiten	45
4.3.3	Einhaltung rechtlicher Rahmenbedingungen	46

4.3.4	Einhaltung spezieller rechtlicher Rahmenbedingungen und Standards.....	47
4.3.5	Umgang mit geänderten Anforderungen und rechtlichen Rahmenbedingungen.....	48
4.3.6	Notfallkonzepte	50
4.3.7	Berichtspflichten, Prüfungs- und Kontrollrechte	53
4.3.8	Folgen der Vertragsbeendigung.....	55
5	Nachweise zur Erfüllung regulatorischer Vorgaben	58
5.1	Übersicht	58
5.2	Umgang mit Prüfzertifikaten.....	58
5.2.1	Bescheinigungen aufgrund gesetzlicher Grundlagen und Vorgaben	58
5.2.2	Bescheinigungen nach Best Practice und Industrie-Standards.....	59
5.2.3	Bescheinigungen aus dem Umfeld der Jahresabschlussprüfung.....	59
5.3	Standardisierung versus Individualisierung der Prüfung: Was treibt die Kosten?	59
5.4	Was leisten einheitliche Zertifikate bereits heute - wo liegen Ziele?	61
6	Datenschutzrechtliche Aspekte.....	63
6.1	Datenschutz bei Funktionsübertragung und Auftragsdatenverarbeitung	63
6.2	Datenübermittlungen oder -verarbeitungen im Ausland	64
7	Fallbeispiele für die Anwendung von Richtlinien, Standards und Referenzmodellen ...	67
7.1	Einführung – zum Erkenntnisgewinn aus Fallbeispielen.....	67
7.2	Fallbeispiel 1 - IT-Sicherheit.....	68
7.2.1	Gesetzliche Anforderungen und Unternehmensdarstellung	68
7.2.2	Ausgangssituation und Überlegung zur Auswahl eines Standards	68
7.2.3	Projekttablauf	71
7.2.4	Zertifizierungsprozess.....	72
7.3	Fallbeispiel 2 - Interne Kontrollprozesse	73
7.3.1	Gesetzliche Anforderungen und Unternehmensdarstellung.....	73
7.3.2	Ausgangslage	73
7.3.3	Projekthalt	73
7.3.4	Corporate Governance Codex	75
7.4	Fallbeispiel 3 - Einführung eines internen IT Kontroll-System	76
7.4.1	Gesetzliche Anforderungen und Unternehmensdarstellung.....	76
7.4.2	Ausgangslage	76
7.4.3	Risiko Mapping.....	77
7.4.4	Einführung interner IT-Kontrollen	77
7.4.5	Fragen bei der Einführung eines internen IT-Kontroll-Systems nach CoBIT.....	78
7.5	Fallbeispiel 4 - Auslagerung eines Rechenzentrums.....	78
8	Glossar.....	79
9	Sachwortverzeichnis.....	98
10	BITKOM-Arbeitskreis Outsourcing.....	105

Abbildung 1: Wertschöpfungsrelevanz der IT.....	15
Abbildung 2: Interne Projektvorbereitung	71
Tabelle 1: Verzeichnis der Abkürzungen	8
Tabelle 2: Arten von (Rechts-)Quellen	20
Tabelle 3: Auswahl IT-Outsourcing relevanter Compliance Regelungen	24
Tabelle 4: Standards mit Möglichkeit zur Zertifizierung von Kontroll-Systemen	34
Tabelle 5: SAS 70 Berichte im Überblick	37
Tabelle 6: Referenzmodelle.....	39
Tabelle 7: Standardisierte oder individualisierte Prüfung - Entscheidungsfaktoren	60
Tabelle 8: Varianten zur Gewährleistung des Datenschutzes	64
Tabelle 9: Kurzprofil des Arbeitskreises Outsourcing	105
Merksatz 1	13
Merksatz 2.....	18
Merksatz 3.....	41
Merksatz 4	58
Merksatz 5.....	63
Merksatz 6	67
Klauselbeispiel 1: Einhaltung der rechtlichen Rahmenbedingungen.....	47
Klauselbeispiel 2: Technische und organisatorische Maßnahmen und Standards	48
Klauselbeispiel 3: Umgang mit geänderten oder neuen rechtlichen Bedingungen	50
Klauselbeispiel 4: Notfälle	52
Klauselbeispiel 5: Berichtspflichten	54
Klauselbeispiel 6: Weisungs-, Prüfungs- und Kontrollrechte.....	54
Klauselbeispiel 7: Exit Management.....	56

Tabelle 1: Verzeichnis der Abkürzungen

AICPA	American Institute of Certified Public Accountants
AK OSC	BITKOM-Arbeitskreis Outsourcing
AktG	Aktiengesetz
AO	Abgabenordnung
ASP	Application Service Providing
BaFin	Bundesanstalt für die Finanzdienstleistungsaufsicht (www.bafin.de)
BAKred	Bundesaufsichtsamt für das Kreditwesen; inzwischen → BaFin
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (www.bitkom.org)
BGH	Bundesgerichtshof
BGHZ	Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BPO	Business Process Outsourcing
BSI	Bundesamts für Sicherheit in der Informationstechnik (www.bsi.de)
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CoBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
D & O	Directors & Officers
DIN	Deutsches Institut für Normung e.V. (www.din.de)
EA	European co-operation for Accreditation (www.european-accreditation.org)
EDV	elektronische Datenverarbeitung
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
ERP	Enterprise Resource Planning
EU	Europäische Union
FAIT	Fachausschuss für Informationstechnologie beim → IDW
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GmbHG	GmbH Gesetz
GoB	Grundsätze ordnungsgemäßer Buchführung

GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
GPSG	Geräte- und Produktsicherheitsgesetz
HGB	Handelsgesetzbuch
HR	Human Resources
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V. (www.idw.de)
IEC	International Electrotechnical Commission (www.iec.ch)
IKS	internes Kontrollsystem
ISACF	Information Systems Audit Control Foundation, inzwischen → IT Governance Institute
ISMS	Informations-Sicherheits-Management-System
ISO	International Organization for Standardization (www.iso.org)
ITGI	IT Governance Institute (www.itgi.org)
ITIL	IT Infrastructure Library
ITK	Informations- und Telekommunikationstechnologie
ITO	IT-Outsourcing
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KVP	kontinuierlicher Verbesserungsprozess
KWG	Kreditwesengesetz
MaRisk	Mindestanforderungen an das Risiko-Management
NJW	Neue Juristische Wochenschrift
OCG	Office of Government Commerce (www.ogc.gov.uk)
RS	Stellungnahme zur Rechnungslegung
RZ	Rechenzentrum
SAS	Statement on Auditing Standards
SEC	Securities and Exchange Commission (www.sec.org)
SLA	Service-Level-Agreement
SMS	Short Message Service
SOX	Sarbanes-Oxley-Act
SSL	Secure Sockets Layer oder auch Secure Server Line
StGB	Strafgesetzbuch
TDG	Gesetz über die Nutzung von Telediensten (Teledienstegesetz)
TGA	Trärgemeinschaft für Akkreditierung GmbH (www.tga-gmbh.de)
TKG	Telekommunikations-Gesetz

TKV	Telekommunikations-Kundenschutz-Verordnung
WpHG	Wertpapierhandelsgesetz
ZIP	führende wirtschaftsrechtliche Fachzeitschrift (Zeitschrift für Wirtschaftsrecht)

1 Executive Summary

IT-Systeme und Prozesse in Unternehmen müssen komplexen gesetzlichen Auflagen entsprechen, die in den letzten Jahren nach spektakulären Firmenzusammenbrüchen deutlich erhöht worden sind. Den daraus erwachsenden Anforderungen müssen sich die Kunden und Anbieter von Outsourcing-Services stellen. Die BITKOM-Publikation „Compliance in IT-Outsourcing-Projekten - LEITFADEN zur Umsetzung rechtlicher Rahmenbedingungen“ greift die brennenden Fragen auf, mit denen sich beide Seiten auseinandersetzen müssen.

Der Leitfaden bietet in den Kapiteln 2 bis 7 eine komprimierte Zusammenstellung der rechtlichen Rahmenbedingungen sowie Hilfestellung zur praktischen Umsetzung. Mit dem Begriff „rechtliche Rahmenbedingungen“ werden dabei nachfolgend alle Gesetze im formellen und materiellen Sinn (z. B. Verordnungen, behördliche Vorgaben und Bekanntmachungen, aufsichtsrechtlicher Anforderungen) sowie Richtlinien und Standards zusammengefasst.

- Kapitel 2 beleuchtet wichtige Zusammenhänge zwischen Compliance, dem Reifegrad der IT-Organisation in einem Unternehmen und den Möglichkeiten der Auslagerung von bestimmten Aufgaben und Geschäftsprozessen, die nicht in der Kernkompetenz von Unternehmen liegen. Ausgehend von der These, dass die Bedeutung von Compliance in vielen Unternehmen noch nicht richtig erkannt wird, argumentieren die Autoren, dass bei geeigneten Rahmenbedingungen ein IT-Outsourcing-Projekt zur Erhöhung des Unternehmenswertes beitragen kann, weil professionelle Service-Provider der Umsetzung von Compliance besonderes Augenmerk schenken.
- Kapitel 3 des Leitfadens beschreibt die wichtigsten gesetzlichen Anforderungen und relevanten Standards mit ihren Geltungsbereichen und bewertet deren Wichtigkeit für IT-Outsourcing-Projekte.
- Kapitel 4 knüpft nahtlos an das Kapitel 3 an. Während dort die rechtlichen und sonstigen Rahmenbedingungen dargestellt werden, beschäftigt sich dieses Kapitel mit den Rechtsfolgen aus der Nichteinhaltung sowie mit der vertraglichen Umsetzung.
- Kapitel 5 erläutert, wie die Outsourcing-Kunden und –Anbietern die Konformität zu Vorgaben und Anforderungen aus rechtlichen Rahmenbedingungen mit bestimmten Nachweisen, Prüfzertifikaten und Bescheinigungen dokumentieren können. Aus der Vielfalt der Zielgruppen solcher Nachweise sowie der Formate für Prüfungen und Ergebnisdarstellungen wird abgeleitet, dass es weder standardisierte Prüfroutinen, noch allgemeingültige Prüfbescheinigungen gibt. Vielmehr orientieren sich Art und Inhalt der Prüfberichterstattung und deren Kosten an den individuellen Anforderungen der Kunden und Anbieter.

- Kapitel 6 geht auf die speziellen Anforderungen bei Offshoring und Nearshoring - also der Verlagerung der Leistungserbringung ins Ausland – ein.
- Kapitel 7 unterstützt den praktischen Bezug des Leitfadens und zeigt an Fallbeispielen einige typische Situationen für die praktische Umsetzung auf. Best Practice bietet aggregierte Erfahrungen und gibt Entscheidungsträgern Anregungen für ihre Outsourcing-Projekte.
- Kapitel 8 + 9 erleichtern die Orientierung in einer komplexen Materie. Das Glossar ist ein Auszug aus den Arbeitsergebnissen der Projektgruppe „Terminologie“.

Der Leitfaden trägt zum Verständnis von zwei grundsätzlichen Erkenntnissen bei:

- Unternehmen treffen eine Entscheidung für IT-Outsourcing zumeist nach wirtschaftlichen Gesichtspunkten. Der ökonomische Vorteil des IT-Outsourcings für den Kunden wird beim Anbieter durch Standardisierung und Zentralisierung von Dienstleistungen geschaffen. Auf diese Weise lassen sich Skaleneffekte erzielen. Der Anbieter schafft damit eine Basis, von welcher auch sein Kunde wirtschaftlich profitiert. Skaleneffekte sind Teil der Wirtschaftlichkeitsrechnung des Dienstleisters und sind in dessen Preisgestaltung berücksichtigt.
- Da Outsourcing-Verträge typischerweise eine mehrjährige Laufzeit haben, ist absehbar, dass es sowohl Änderungen der rechtlichen Rahmenbedingungen als auch der Anforderungen seitens des Kunden geben wird, die zum Zeitpunkt des Vertragsabschlusses nicht absehbar waren. Dies kann und wird zu der Situation führen, dass sich die Wirtschaftlichkeitsbetrachtung seitens des Kunden und des Anbieters im Nachhinein anders als geplant darstellt. Die Praxis zeigt andererseits, dass es ein realitätsfernes Unterfangen ist, alle möglichen Änderungen vertraglich festzuschreiben zu wollen. Es ist daher wichtig, im Outsourcing-Vertrag Mechanismen und Regelungen festzulegen, die den Umgang mit solchen Änderungen ermöglichen und somit die notwendige vertragliche Flexibilität schaffen, auf neue Anforderungen so einzugehen, dass sie sich für beide Vertragsparteien wirtschaftlich sinnvoll darstellen lassen.

Wegen des begrenzten Rahmens kann der Leitfaden nicht auf spezifische Industrie- oder Branchenanforderungen eingehen. Interessanterweise zeigt die Erfahrung der BITKOM-Mitglieder, dass gerade das industriespezifische Wissen häufiger vorhanden ist als die im Leitfaden aufgearbeiteten generellen Kenntnisse.

Der Leitfaden spiegelt den Erkenntnisstand wider, der mit dem Abschluss seiner Ausarbeitung im Juli 2006 erreicht wurde. Er erhebt keinen Anspruch auf Vollständigkeit, kann aufgrund der Vielfalt der behandelten Fragestellungen und der fortlaufenden Entwicklung des Rechts nur Empfehlungscharakter tragen und eine individuelle rechtliche Beratung nicht ersetzen.

2 Compliance, Reifegrad einer IT-Organisation und Outsourcing

Merksatz 1

Die Bedeutung von Compliance wird in vielen Unternehmen noch nicht richtig erkannt. Bei geeigneten Rahmenbedingungen wird ein IT-Outsourcing-Projekt zur Erhöhung des Unternehmenswertes beitragen, da Service-Provider im Interesse eigener Wettbewerbsfähigkeit die Umsetzung von Compliance professionell gewährleisten müssen.

2.1 Bedeutung von Compliance in Outsourcing-Entscheidungen

Was haben die in diesem Leitfaden beschriebenen rechtlichen Rahmenbedingungen in Bezug auf IT-Outsourcing gemeinsam, wie kann ein Unternehmen seine Informationstechnologie im Hinblick auf ihren aktuellen Erfüllungsgrad der Vorgaben optimieren? Und wie kann ein Vertragswerk über ein Outsourcing-Projekt im Interesse von Kunde und Anbieter von unnötiger Komplexität freigehalten werden?

Compliance zielt darauf ab, die Sicherheit und das Risiko eines Unternehmens und damit auch der IT zu optimieren und so den Fortbestand der Unternehmung zu gewährleisten. Im Rahmen der Auftragsdatenverarbeitung, der üblichen Form des IT-Outsourcing, verbleibt dabei die Verantwortung für die Einhaltung der Vorgaben an Ordnungsmäßigkeit und Sicherheit des IT-Betriebs sowie die Sicherheit der Daten bei der Geschäftsführung des auslagernden Unternehmens (vgl. S. 43).

Im Hinblick auf Outsourcing-Entscheidungen ist deshalb zunächst in erster Linie eine Einschätzung der Erfüllung rechtlicher Rahmenbedingungen im eigenen Unternehmen relevant. Outsourcing kann einen wesentlichen Beitrag leisten, den Erfüllungsgrad positiv zu beeinflussen.

Im Outsourcing – wie in anderen Bereichen auch – lässt sich die Risikobetrachtung auf die wesentlichen Aspekte Kontrolle der Ordnungsmäßigkeit, Datenschutz und Sicherheit zusammenfassen. Im Zusammenhang mit Outsourcing verändert sich allerdings der Fokus insbesondere auf die Prüfung der Durchgängigkeit der Kontrolle. Beim Outsourcing muss nämlich insbesondere gewährleistet sein, dass Kontrollmechanismen zur Prüfung

- der Ordnungsmäßigkeit der *externen* Durchführung,
 - die Einhaltung des Datenschutzes und
 - die Gewährleistung der Sicherheit
- existieren.

Welche Bedeutung haben diese Zusammenhänge für eine Sourcing-Entscheidung?

Auf strategischer Ebene wird in vielen deutschen mittelständischen Unternehmen die Rolle der IT und ihr Beitrag zum Unternehmenserfolg kritisch hinterfragt. Die Form des traditionellen IT-Betriebs mit dem Fokus auf die unternehmensinterne Verarbeitung von Daten reicht in der schnell fortschreitenden Globalisierung der Wirtschaft nicht mehr aus, um der zunehmenden prozessuralen Vernetzung in der Supply Chain zwischen Kunden und Lieferanten Rechnung zu tragen.

Die IT-Organisationen müssen in eine neue Rolle schlüpfen und im eigenen Unternehmen beratend dazu beitragen, die Effizienz und Effektivität von Geschäftsprozessen zu steigern und damit die Wertschöpfung zu erhöhen. Auch im Mittelstand entwickeln sich deshalb zunehmend strukturierte IT-Organisationsmodelle für die Umsetzung der neuen Anforderungen. Es reift die Erkenntnis, dass die eigentliche Kernkompetenz einer modernen Unternehmens-IT in den Prozesskenntnissen und nicht im Betrieb von Rechenzentren und Infrastruktur liegt.

Genau auf die Prozesse zielen aber der im Kapitel 3 beschriebene Schutz und die Kontrolle durch Gesetze, Richtlinien und Standards. Die IT, die die operative Umsetzung der Prozesse ermöglicht, ist also direkt betroffen und unterliegt in jedem Fall – ob ausgelagert oder nicht – dem Fokus der Wirtschaftsprüfung. Problematisch dabei ist heute im Allgemeinen der Stand der Umsetzung in den Unternehmen¹.

Sowohl für die Geschäftsführung als auch für die Wirtschaftsprüfung bedeutet das: Die Bewertung der Risiken des Unternehmens ist auch im Hinblick auf eine Outsourcing-Entscheidung relevant. Je nach ihrem Reifegrad ist nämlich die interne Unternehmens-IT mehr oder weniger in der Lage, die regulatorischen Anforderungen tatsächlich zu erfüllen.

Generell sind die Beweggründe der Auseinandersetzung mit IT-Outsourcing sehr unterschiedlich. Vor dem Hintergrund regulatorischer Vorgaben spielen die Risikobeherrschung und die Sicherheit als Outsourcing-Motive zurzeit im Markt nur eine untergeordnete Rolle. Compliance gewinnt aber aufgrund des zunehmenden Drucks internationaler Vorgaben (z.B. SOX) rasant an Bedeutung. Auch wenn deutsche mittelständische Unternehmen nicht direkt den Vorgaben von SOX unterliegen, so interessieren sich die internationalen Kunden des Exportweltmeisters Deutschland immer mehr auch für die internen Prozesse ihrer Lieferanten. Daher ordnet sich Compliance als neuer Aspekt nahtlos in die allgemeinen Überlegungen für eine Outsourcing-Entscheidung ein:

¹ "Erfahrungsgemäß ist die Qualität und Zuverlässigkeit der Informations-Sicherheit als unzureichend einzuschätzen. Selbst dort, wo es formalisierte Sicherheitsprozesse gibt, ist die Wirksamkeit dieser Prozesse im Vergleich zu anerkannten Standards (ISO, BSI, FAIT) und sonst relevanter gesetzlichen Vorgaben (GoB, AO, KWG, BaFin, u.v.m.) häufig als unzureichend zu bewerten", so Robert Chapman, für Information Security in Deutschland zuständiger Partner (CISM, CISA), KPMG, Advisory, auf dem BITKOM-Forum „Outsourcing und Sicherheit“ am 29. Juni 2006.

Es geht um Kostensenkung und Qualitätssteigerung und damit um die Umsetzung der strategischen Ziele des Unternehmens mit Hilfe der IT.

2.2 Wertschöpfung der IT und ihrer auszulagernden Teile

Zur Strukturierung der Motive für Outsourcing ist die Abbildung 1 hilfreich. In praktischen Situationen bewegen sich Entscheidungsträger zwischen den beiden „Extremen“ Kosten- bzw. Wertschöpfungs-Fokus und spiegeln dabei auch den Stand bei der Umsetzung rechtlicher Rahmenbedingungen wider:

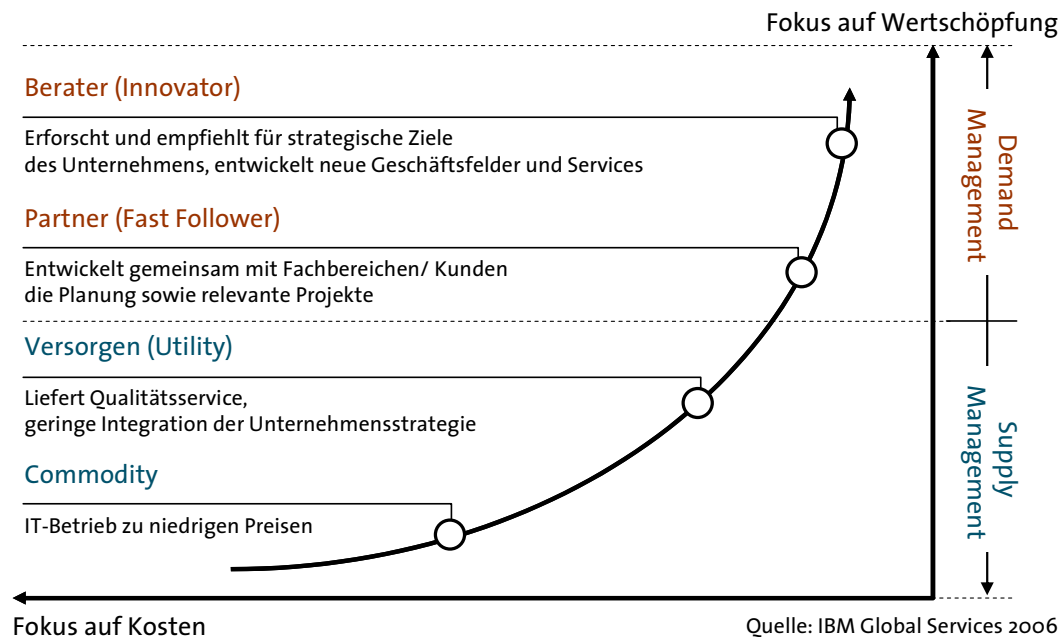


Abbildung 1: Wertschöpfungsrelevanz der IT

- Im ersten Extremfall, beim „Fokus auf den Kosten“, herrscht die Sicht auf die Unternehmens-IT als reine Technikabteilung („Commodity“). Wenn eine IT-Organisation so wahrgenommen wird, dann hat sie es offensichtlich versäumt, ihren Beitrag zur Wertschöpfung und zum Unternehmenserfolg zu entwickeln oder vielleicht auch nur richtig darzustellen. Eine solche IT-Organisation benötigt einen Großteil der Ressourcen zur Aufrechterhaltung des allgemeinen Betriebs und zur Bewältigung der wichtigsten Projekte. Für die Umsetzung gesetzlicher und prüfungsrelevanter Anforderungen reichen meist weder Zeit noch Geld. In den Augen der Geschäftsführung stellt die IT lediglich einen Kostenfaktor dar, der durch Outsourcing in Preis und Qualität optimiert werden kann.
- Beim „Fokus auf der Wertschöpfung“, dem anderen Ende des Kontinuums, ist eine IT-Organisation angesiedelt, die bereits den Wandel zum internen Berater mit Prozesskompetenz vollzogen hat. Sie kann durch aktive Prozessberatung und –gestaltung einen wesentlichen Beitrag zur Wertschöpfung des Unternehmens leisten und betreibt in vielen Fällen bereits ein aktives Sourcing.

Der Grad der Standardisierung und Automatisierung im reinen IT-Betrieb hat ein Niveau erreicht, das aus prüfungsrelevanten Gesichtspunkten keinen Anlass für Veränderung bietet. Aufgrund des geringen Beitrags zur Wertschöpfung des Unternehmens wird der reine Betrieb von IT und damit ein Teil der Umsetzung (nicht Kontrolle!) der rechtlichen Rahmenbedingungen aber nicht als Kernkompetenz der unternehmensinternen IT-Organisation gesehen und ausgelagert. Die verbleibende IT-Organisation entwickelt eine neue Kompetenz, die Kontrolle der Umsetzung, die weniger aufwändig ist als die Umsetzung, und trägt so aktiv zur Minderung nicht-wertschöpfender Aktivitäten des Unternehmens bei.

Unabhängig vom Wertschöpfungsgrad der IT in einem Unternehmen kann Outsourcing einen Beitrag zur Erhöhung der Wettbewerbsfähigkeit leisten: Professionelle Dienstleister unterstützen bei der besseren Erfüllung regulatorischer Standards, und die Auslagerung nicht unmittelbar wertschöpfender Aufgaben wie der Risikominimierung im IT-Betrieb spart Ressourcen.

Die vertragliche Abbildung des Outsourcings wird sich je nach Grad der Wertschöpfung der auszulagernden Komponenten unterscheiden.

2.3 Das Risiko auslagern?

Gut geplantes IT-Outsourcing kann sehr wohl dazu beitragen, die Komplexität der Risikokontrolle zu reduzieren. In den Fällen, in denen die Ordnungsmäßigkeit des Dienstleistungs-Unternehmens geprüft werden muss, kann nämlich auf Ergebnisse der Prüfung zurückgegriffen werden, die der Abschlussprüfer des Dienstleistungs-Unternehmens vornimmt. Standards wie SAS 70 (vgl. Tabelle 4) helfen zusätzlich, die Komplexität einer Outsourcing-Beziehung im Hinblick auf die Kontrollmechanismen zu reduzieren (vgl. S. 34).

Was bedeutet das für den Kunden? Für sich gesehen ändert eine Auslagerung von IT in der Regel nicht die rechtlichen Rahmenbedingungen des auslagernden Unternehmens. IT-Outsourcing stellt damit nicht direkt eine Option zur Verlagerung von Verantwortlichkeiten auf Dritte und damit automatisch die Minimierung des Gesamtrisikos für ein Unternehmen dar. Dennoch kann die Verlagerung des IT-Betriebs prüfungsrelevante und damit auch kostenrelevante Aspekte mit sich bringen, die gerade für mittelständische Unternehmen erhebliche Potenziale bergen können:

- Die verbleibende eigenen IT-Organisation kann einen Wandel hin zum internen Prozessberater und zur Kontrollinstanz vollziehen.
- Die Kontrolle des Risikos „IT-Betrieb“ wird ausgelagert.
- Es verbleibt die Kontrolle, die gleichzeitig die Konzentration der IT-Organisation auf Geschäftsprozesse erhöht und die auch damit mehr zum kontinuierlichen Verbesserungsprozess beitragen kann.
- Die Qualität der Leistung kann gesteigert werden.
- Die von der IT eingesparten Kosten können wertschöpfend im Prozessumfeld und damit in der eigentlichen Kernkompetenz der IT-Organisation investiert werden.

Der z.B. mit Furcht vor Kontrollverlust motivierte Verzicht darauf, Outsourcing als Option zur Verbesserung des Wertbeitrags der IT-Organisation zu prüfen, bedeutet oft die Fortsetzung von erheblichen Investitionen in „unproduktive“ Bereiche von IT. Gerade in mittelständischen Unternehmen wird IT im Allgemeinen noch immer als Kostenfaktor gesehen. Das grenzt per se die Flexibilität der IT stark ein, denn erfahrungsgemäß stehen die eigentlich erforderlichen personellen und finanziellen Ressourcen im Mittelstand oft nicht zur Verfügung. Dass die Auslagerung des IT-Betriebs eine sinnvolle Entscheidung darstellen kann, zeigt sich nicht zuletzt auch in der Tatsache, dass sich der Lebenszyklus von IT-Systemen ähnlich schnell verkürzt wie sich die Zahl der Vorschriften für einen ordnungsgemäßen IT-Betrieb vermehrt.

Durch das IT-Outsourcing hat der Kunde keinen unmittelbaren Einfluss mehr auf die IT. Obwohl IT in den meisten Unternehmen keine Kernkompetenz darstellt, so ist IT ein essentielles Herzstück, mit dem die Funktionsfähigkeit eines Unternehmens und damit seine Wettbewerbsposition am Markt beeinflusst werden kann. Die sich aus diesem Spannungsfeld ergebenden Risiken werden insbesondere in den Gesetzen KonTraG, SOX, BDSG, KWG, Basel II, BaFin usw. (vgl. Kapitel 3) angesprochen, die während eines Outsourcing-Projektes ein striktes Risiko-Management erfordern.

Aus diesem Spannungsfeld heraus haben Anbieter der Outsourcing-Leistung und der Kunde die gemeinsame Aufgabe, zu Beginn des Projektes die Risiken für beide Seiten zu identifizieren.

3 Vorschriften und Standards im Outsourcing

Merksatz 2

Im Zusammenhang mit IT-Outsourcing-Projekten wird heutzutage eine kaum zu überblickende Vielzahl von Anforderungen gestellt, die sich aus gesetzlichen Regelungen, Richtlinien und relevanten Standards sowie Referenzmodellen ergeben. Die Anforderungen betreffen auch die Verantwortung der Geschäftsführung eines Unternehmens in Bezug auf Handlungs- und Haftungsverpflichtungen für ausgelagerte Prozesse. Werden bestimmte Aufgaben oder Geschäftsprozesse an ein Dienstleistungs-Unternehmen ausgelagert, so verbleibt die Verantwortung für deren ordnungsgemäße, sichere und gesetzeskonforme Abwicklung bei der Geschäftsführung des Auftraggebers.

3.1 Einführung

Im Zusammenhang mit IT-Outsourcing-Projekten wird heutzutage eine kaum zu überblickende Vielzahl von rechtlichen Anforderungen gestellt, die sich aus Quellen unterschiedlichster Art, mit mehr oder weniger hoher Verbindlichkeit und vielfältigen Konsequenzen ergeben.

Dabei sollte im Sinne einer effizienten Umsetzungsstrategie danach unterschieden werden, welche Regelungen

- allgemeingültig und damit zwingend zu beachten sind,
- welche nur einen mittelbaren (faktischen) Zwang entfalten² oder
- gegebenenfalls keiner weiteren intensiven Beachtung bedürfen.

Regelungen mit „Gesetzescharakter“³ gelten gegenüber jedermann. Andere Anforderungen dienen - auf den ersten Blick - lediglich als Richtschnur, können aber „über Umwege“ Verbindlichkeit erhalten, z.B. wenn ein Gesetz dies anordnet oder wenn sich ein Sicherheitsstandard in einer Branche so durchgesetzt hat, dass dessen Nichtbeachtung negative Folgen haben könnte⁴. Um Unternehmen im Dickicht der Regelungen diese Differenzierung zu erleichtern, soll die Rechtsnatur der verschiedenen Regelungen einschließlich ihrer Wirkung (oder „Verbindlichkeitsstufe“) kurz abstrakt und mit Beispielen erläutert werden. Die Tabelle 2 gibt einen Überblick über Regelungen, die im Rahmen von Outsourcing-Vorhaben Anwendung finden können, jedoch

² z.B. da ihre Missachtung wirtschaftliche Nachteile nach sich ziehen könnte.

³ Nach Art. 2 Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB) ist „Gesetz“ im Sinne des Bürgerlichen Gesetzbuchs jede Rechtsnorm. Rechtsnormen sind Regeln, die eine abstrakt-generelle Geltung und Außenwirkung haben, d.h. die jeder beachten muss.

⁴ z.B. im Gerichtsverfahren bei der richterlichen Beweiswürdigung.

stellen die dargestellten Kategorien weder Gegensatzpaare dar, noch ist deren Aufzählung abschließend.

Die gesetzlichen Regelungen, Richtlinien und relevanten Standards in diesem Leitfaden wurden speziell unter Betrachtung eines besonderen Bezugs zu Outsourcing-Projekten ausgewählt (vgl. auch Tabelle 3). Sie betreffen u.a. die Verantwortung der Geschäftsführung eines Unternehmens in Bezug auf Handlungs- und Haftungsverpflichtungen für die ausgelagerten Prozesse und geben Anhaltspunkte zur effektiven Gestaltung und Kontrolle der Outsourcing-Beziehung.

Wird ein Geschäftsprozess oder eine bestimmte Aufgabe an ein Dienstleistungs-Unternehmen ausgelagert, so verbleibt die Verantwortung für die ordnungsgemäße, sichere und gesetzeskonforme Abwicklung dieses ausgelagerten Prozesses im eigenen Unternehmen, also bei der Geschäftsführung.

Grundsätzlich lassen sich die rechtlichen Rahmenbedingungen wie folgt strukturieren:

- Gesetzliche Regelungen bleiben üblicherweise eher allgemein, da sie eine Vielzahl von Situationen regeln und letztlich nur das Endziel vorgeben wollen.
- Richtlinien weisen hingegen meistens die Handschrift von Praktikern auf und beziehen Handlungsempfehlungen ein.
- Standards enthalten die am konkretesten formulierten Vorgaben und entstehen in der Regel im Konsens der jeweiligen Interessengruppen.

Die Tabelle 2 gibt einen Überblick über die unterschiedlichen rechtlichen Rahmenbedingungen.

Tabelle 2: Arten von (Rechts-)Quellen

Quelle	Definition	Wirkung	Beispiele
Formelles Gesetz	Gesetze, die in einem parlamentarischen Verfahren zustande gekommen sind	Abstrakt-generell auf Herbeiführung einer Rechtsfolge gerichtet (unmittelbare Außenwirkung gegenüber jedermann)	Europäisches Primärrecht (z.B. EG-Vertrag) ⁵ Europäisches Sekundärrecht (Verordnungen und Richtlinien) Nationale Bundes- und Landesgesetze (z.B. KWG, BDSG, Landesdatenschutzgesetze, gesellschaftsrechtliche Bestimmungen wie z. B. § 91 II AktG)
Gesetze im materiellen Sinn, insbesondere Rechtsverordnungen	Gesetze, die aufgrund einer Ermächtigungsnorm in einem formellen Gesetz von der Verwaltung (z.B. Minister) erlassen werden	Abstrakt-generell auf Herbeiführung einer Rechtsfolge gerichtet	Telekommunikationskundenschutzverordnung (TKV) aufgrund von § 45 TKG 2004

⁵ Internationale (völkerrechtliche) Verträge, die über die EU hinausgehen, binden in der Regel nur Staaten und entfalten keine unmittelbare Wirkung zwischen Privaten.

Quelle	Definition	Wirkung	Beispiele
Richtlinien, Rundschreiben, Empfehlungen, Verlautbarungen und Bekanntmachungen der Verwaltung	Allgemeine Äußerungen der Verwaltung, die unter anderem Gesetze auslegen, konkretisieren und die Rechtsauffassung der Verwaltung zu bestimmten Fragen wiedergeben	Abstrakt-generell, aber keine unmittelbare rechtliche Außen- und Bindungswirkung	Rundschreiben 11/2001 des BAKred ⁶ zur Auslagerung von Bereichen auf ein anderes Unternehmen Rundschreiben 18/2005 der BaFin zu den Mindestanforderungen an das Risiko-Management (MaRisk) BSI-Grundschutzhandbuch
Verwaltungsakte	Hoheitliche Entscheidung einer Behörde auf dem Gebiet des öffentlichen Rechts zur Regelung eines Einzelfalles mit Außenwirkung	In der Regel konkret-individuell (berechtigten und verpflichten nur den Adressaten)	Erteilung einer Erlaubnis zum Betrieb von Bankgeschäften oder Finanzdienstleistungen gem. § 32 KWG
Standards	Privatrechtlich (häufig von Interessenverbänden) ausgehandelte Regelungen, häufig technischer Art	In der Regel freiwillige Selbstverpflichtung, Bindungswirkung nur mittelbar ⁷ Standards können insbesondere bei der Bestimmung des anzuwendenden Sorgfaltsmaßstabs bedeutsam werden.	Corporate Governance Codex DIN oder ISO-Normen

⁶ Bundesaufsichtsamt für das Kreditwesen; jetzt Bundesanstalt für die Finanzdienstleistungsaufsicht (BaFin).

⁷ z.B. soweit ein formelles Gesetz die Anwendung vorschreibt oder zwischen Vertragspartnern oder durch Branchenübung.

Zusätzlich zu den rechtlichen Rahmenbedingungen sind in diesem Leitfaden auch einige Rahmen- oder Referenzmodelle (vgl. Abschnitt 3.6) dargestellt, die in den letzten Jahren von privaten Interessengruppen⁸ oder regierungsnahen Instituten im angelsächsischen Raum⁹ entwickelt wurden.

Diese Referenzmodelle dienen einer höheren Effizienz bei der Einführung von IT-Kontrollmaßnahmen im Unternehmensumfeld. In der Regel sind Referenzmodelle wie z.B. CoBIT oder ITIL an Gesetze, Richtlinien oder Standards angelehnt und versuchen den Brückenschlag über eine Vielzahl solcher Regelungen. CoBIT und ITIL sind mittlerweile international anerkannte und angewandte Modelle. Das CoBIT-Referenzmodell stellt dabei einen Leitfaden für die Durchführung von Kontroll- und Führungsaufgaben im Rahmen der IT-Governance dar, während ITIL stärker auf operative Aufgaben ausgerichtet ist und sich detailliert mit dem IT-Service-Management beschäftigt.

3.2 Relevanz für IT-Outsourcing

Seit dem Einzug der IT in nahezu alle Unternehmen hat sich ihr Stellenwert für den Geschäftserfolg stetig erhöht. So wird es nicht verwundern, dass sich mit einem gesteigerten Wertbeitrag der IT auch die Verantwortung der Geschäftsführung für ihren effizienten Einsatz und problemfreien Betrieb erhöht hat. Die notwendige Übernahme dieser Verantwortung schlägt sich mittlerweile in zahlreichen gesetzlichen und privatwirtschaftlichen Vorgaben nieder, mit denen sich die Geschäftsleitungen von Unternehmen in Deutschland auseinander setzen müssen.

Für die Darstellung im vorliegenden Leitfaden haben sich die Autoren auf diejenigen Gesetze, Richtlinien, Standards und Referenzmodelle beschränkt, die in direktem oder indirektem Zusammenhang mit der Auslagerung bestimmter IT-Dienstleistungen stehen bzw. generell einen Bezug zum Management von IT-Dienstleistungen haben.

Wegen des begrenzten Rahmens kann der Leitfaden nicht auf spezifische Industrie- oder Branchenregelungen eingehen, z.B. Anforderungen, die sich aus dem KWG¹⁰ oder dem WpHG ergeben.

⁸ wie z.B. dem IT Governance Institute (www.itgi.org).

⁹ wie z.B. dem Office of Government Commerce (OGC, vormals Central Computer and Telecommunications Agency).

¹⁰ § 25a Absatz 1 Kreditwesengesetz (KWG) gibt besondere organisatorische Anforderungen an Kredit- und Finanzdienstleistungs-Institute vor, wozu z.B. die Schaffung angemessener Sicherheitsvorkehrungen für den EDV-Einsatz gehört. In § 25a Absatz 2 KWG ist für den Fall des Outsourcings festgelegt, dass im Rahmen der Auslagerung von Bereichen auf ein anderes Unternehmen, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen, noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung, noch die Prüfungsrechte und Kontrollmöglichkeiten der Bundesanstalt für

Obwohl der besondere Bezug zum IT-Outsourcing bei einigen Gesetzen, Richtlinien und Standards in der Tabelle 3 eher als „niedrig“ eingestuft wurde, bedeutet das natürlich nicht, dass sich die Unternehmensleitung mit diesen Regelungen nicht auseinandersetzen muss. Im vorliegenden Leitfaden belässt es das Autorenteam deshalb auch bei dem Ansatz, die Anforderungen der IT-Governance strukturiert und fokussiert mit dem Thema IT-Outsourcing zu verbinden. Der Fokus liegt in den nachfolgenden Abschnitten also zunächst einmal auf Regelungen, deren Bezug zum IT-Outsourcing in der Tabelle 3 mit „hoch“ oder „mittel“ bewertet wurde.

Steuerliche Aspekte, die bei der Auslagerung von Dienstleistungen und der Anwendung bestehender Steuergesetze entstehen, sind nicht Gegenstand des Leitfadens. Die Komplexität des Steuerrechts und dessen Anwendung auf unterschiedliche Individualfälle sind dafür wesentliche Beweggründe. Gleiches gilt für arbeitsrechtliche Fragestellungen, z.B. Rechtsfragen eines Betriebsübergangs bei einem IT-Outsourcing.

Auch versicherungsrechtliche Aspekte sind im Rahmen von IT-Outsourcing-Projekten zu beachten; schließlich ist die Unterhaltung geeigneter IT-Sicherheits- und Schutzvorkehrungen nach vielen Versicherungsverträgen Voraussetzung für Ansprüche aus der Versicherung, z.B. über entsprechende Obliegenheiten oder Ausschlüsse im Versicherungsvertrag. Da es in diesen Vertragsregelungen aber immer um individuelle Anforderungen geht, wird in diesem Leitfaden auf die versicherungsrechtlichen Aspekte lediglich unter dem Gesichtspunkt der Haftung und der Vertragsgestaltung eingegangen (vgl. Kapitel 4).

Finanzdienstleistungsaufsicht (BaFin) beeinträchtigt werden dürfen. Gemäß § 25 Abs. 2 S. 3 KWG hat die auslagernde Bank der BaFin und der Deutschen Bundesbank sowohl die Absicht als auch den Vollzug des Vorhabens unverzüglich anzuzeigen.

Tabelle 3: Auswahl IT-Outsourcing relevanter Compliance Regelungen

Eine Auswahl IT-Outsourcing relevanter Compliance-Regelungen				
	Ursprung			Besonderer Bezug zum IT-Outsourcing
	D	USA	Global	
Gesetzliche Regelungen				
KonTraG	☒			●●
GmbHG	☒			●●
HGB	☒			●●
Abgabenordnung	☒			●
BDSG	☒			●●●
Sarbanes-Oxley-Act		☒		●●
Richtlinien				
GDPdU	☒			●●
Basel II			☒	●
Standards				
Buchführung				
GoB und GoBS	☒			●●
Wirtschaftsprüfung				
IDW RS FAIT 1	☒			●
IDW PS 330	☒			●●
Zertifizierung von IT-Prozessen				
SAS 70		☒		●●●
IDW PS 331	☒			●●●
BSI-Grundschutz	☒			●●
ISO 17799	☒			●●
Qualität				
ISO 9001:2000			☒	●●
Referenzmodelle				
COSO			☒	●
CoBIT			☒	●●●
ITIL			☒	●●●

Legende:

- Hoch
- Mittel
- Niedrig
- ☒ zutreffend

3.3 Kurze Darstellung der einschlägigen gesetzlichen Regelungen

3.3.1 Auswahlkriterien

Gesetzliche Regelungen sind von Trägern der öffentlichen Hand vorgegeben und für die jeweilige Zielgruppe verbindlich. Aus der Fülle der Gesetze sind diejenigen zu identifizieren, die sich auf die Geschäftsführung eines Unternehmens beziehen und die mit den Verpflichtungen der Geschäftsführung in Bezug auf auszulagernde oder schon ausgelagerte Dienstleistungen zu tun haben (vgl. Tabelle 3). Nur solche Gesetze werden in diesem Leitfaden dargestellt.

3.3.2 Gesetz zur Kontrolle und Transparenz - Haftungsregelung

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) stellt (erweiterte) Forderungen an das Risiko-Management eines Unternehmens und statuiert über § 91 Abs. 2 AktG die rechtlich verbindliche Pflicht der Geschäftsleitung¹¹, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“¹². Gemäß § 317 Abs. 4 HGB hat sich der Abschlussprüfer bei börsennotierten Aktiengesellschaften im Rahmen der Jahresabschlussprüfung von der Existenz eines derartigen Überwachungssystems zu überzeugen und bei der Lageberichterstattung auch den Inhalt dieses Systems und seine Aussagekraft zu beurteilen.

Die Bedeutung des KonTraG bei der Auslagerung von bestimmten Dienstleistungen ist in der erhöhten Pflichtenanspannung für Vorstand, Aufsichtsrat und Wirtschaftsprüfer im Unternehmen zu sehen. Die Vorschriften des KonTraG zwingen die Unternehmensleitung zur Einführung eines unternehmensweiten Risiko-Management-Systems. Da ausgelagerte Dienstleistungen in der Regel im Verantwortungsbereich der Unternehmensleitung verbleiben, müssen im Rahmen des Risiko-Management-Systems geeignete Maßnahmen getroffen werden, um die Einhaltung rechtlicher Rahmenbedingungen sowie bestehender Unternehmensrichtlinien im Hinblick auf das

¹¹ Über Ausstrahlungswirkung gilt diese nach allgemeiner Meinung auch für GmbH, KG und OHG: Nach allgemeiner Meinung ist § 91 Abs. 2 AktG jedenfalls sinngemäß auch auf andere Gesellschaftsformen anwendbar. Vgl. insoweit auch die Begründung zum Regierungsentwurf (BT-Drucks. 13/9712, S. 15): „Es ist davon auszugehen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, Komplexität, ihrer Struktur usw. nichts anderes gilt und die Neuregelung Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat.“

¹² Zwar hat die Geschäftsleitung grundsätzlich Ermessen hinsichtlich der Ergreifung „geeigneter Maßnahmen“, doch spielen hier Standards und Normen eine wichtige Rolle. So sollte auch eine effiziente Strategie zum Umgang mit Informationen im Unternehmen gefunden werden (z.B. Trennung interner von geschäftlichen Informationen), sogenanntes Information-Lifecycle-Management.

Risiko-Management-System auch durch den Outsourcing-Anbieter regelmäßig überprüfen zu können¹³.

3.3.3 GmbH Gesetz – Sorgfaltspflicht und Ordnungsmäßigkeit

Das GmbH Gesetz (GmbHG) regelt in Deutschland im Wesentlichen die besondere Form der Gesellschaft mit beschränkter Haftung (GmbH), ihre Errichtung, ihre Organe und ihre Stellung im Rechtsverkehr.

Im Zusammenhang mit einer Outsourcing-Beziehung erlangt die Pflicht der Geschäftsführer nach dem GmbHG, in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden¹⁴ sowie für die ordnungsmäßige Buchführung der Gesellschaft zu sorgen¹⁵, besondere Relevanz. Dies gilt insbesondere, wenn Teile der Buchhaltung oder sogar die gesamte Buchhaltung an einen Dritten ausgelagert werden. Die Geschäftsführung muss bei der Vergabe von Buchhaltungs-Dienstleistungen an Dritte jederzeit sicherstellen und überprüfen können, ob die Buchhaltung vom Dienstleister ordnungsgemäß (vgl. dazu Abschnitt 3.5.1) durchgeführt wird.

3.3.4 Handelsgesetzbuch – Überprüfung ausgelagerter Buchführung

Das Handelsgesetzbuch (HGB) stellt die wesentliche Grundlage für das deutsche Handelsrecht dar. Den direkten Bezug zu Vorschriften, die das Auslagern von Dienstleistungen betreffen, wird man im HGB vergeblich suchen. Jedoch gibt es auch hier einige Vorschriften, die die Verpflichtungen des Kaufmanns darlegen. So wird z.B. die Buchführungspflicht speziell in HGB § 238 erwähnt. Die Buchführung muss demnach so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann, und sie muss den Grundsätzen ordnungsgemäßer Buchführung (GoB) entsprechen (vgl. Abschnitt 3.5.1).

Die Anforderungen der §§ 238, 239 und 257 HGB sind bei der Gestaltung einer IT-gestützten Rechnungslegung zu beachten. Im Einzelnen sind dies:

- die Beachtung der Grundsätze ordnungsgemäßer Buchführung (§ 239 Abs. 4 HGB) und
- die Berücksichtigung der damit verbundenen Anforderungen an die Sicherheit IT-gestützter Rechnungslegung,
- die Nachvollziehbarkeit der Buchführungs- bzw. Rechnungslegungsverfahren (§ 238 Abs. 1 Satz 2 HGB),

¹³ z.B. durch eine Interne Revision.

¹⁴ siehe GmbHG § 43.

¹⁵ siehe GmbHG § 41.

- die Nachvollziehbarkeit der Abbildung der einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung (§ 238 Abs. 1 Satz 3 HGB),
- die Einhaltung der Aufbewahrungsvorschriften (§ 239 Abs. 4, § 257 HGB).

Sind Teile der Buchhaltung an einen Dritten ausgelagert, müssen demnach Vorkehrungen getroffen werden, die Einhaltung der GoB auch für die ausgelagerten Prozesse, sofern rechnungslegungsrelevant¹⁶, regelmäßig überprüfen zu können. In HGB §§ 316 - 324 werden die entscheidenden Vorgaben für den Abschlussprüfer der betroffenen Gesellschaft aufgeführt. Der Abschlussprüfer hat - laut Gesetz „mit der gebotenen Klarheit“ - über die Lage des Unternehmens zu berichten.

3.3.5 Bundesdatenschutzgesetz - Verarbeitung personenbezogener Daten¹⁷

Bei IT-Outsourcing-Projekten sind regelmäßig auch datenschutzrechtliche Aspekte zu beachten, sofern personenbezogene Daten von der Outsourcing-Maßnahme betroffen sind. Als solche gelten gemäß § 3 Abs. 1 BDSG alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Das BDSG wurde im Jahr 2002 an die EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995²⁰ angepasst. Ziel der EU-Richtlinie ist die Herstellung eines einheitlichen Datenschutzniveaus in den EU-Mitgliedsstaaten.

Personenbezogene Daten dürfen gemäß § 4 Abs. 1 BDSG nur dann erhoben, verarbeitet und genutzt werden, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

¹⁶ Die Elemente des IT-Systems sind rechnungslegungsrelevant, wenn sie dazu dienen, Daten über Geschäftsvorfälle oder betriebliche Aktivitäten zu verarbeiten, die entweder direkt in die IT-gestützte Rechnungslegung einfließen oder als Grundlage für Buchungen dem Rechnungslegungssystem in elektronischer Form zur Verfügung gestellt werden (rechnungslegungsrelevante Daten). Der Begriff der Rechnungslegung umfasst dabei die Buchführung, den Jahresabschluss und den Lagebericht bzw. auf Konzernebene den Konzernabschluss und den Konzernlagebericht.

¹⁷ Im Web ist unter http://www.bitkom.org/de/publikationen/38337_39321.aspx eine ausführliche Darstellung zur „Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer“ verfügbar.

¹⁸ Gemäß § 3 Absatz 1 BDSG handelt es sich bei personenbezogenen Daten um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

¹⁹ Gemäß der Anlage zu § 9 BDSG insbesondere: Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen und die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies gilt über § 11 BDSG auch für Auftragsdatenverarbeiter.

²⁰ EU-Datenschutzrichtlinie 95/46/EG.

Bei IT-Outsourcing-Maßnahmen stellt sich in der Regel die Frage, ob dem Outsourcing-Anbieter oder beim auslagernden Unternehmen die datenschutzrechtlichen Voraussetzungen gegeben sein müssen. Dies hängt maßgeblich davon ab, ob die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch den Outsourcing-Anbieter im Rahmen einer so genannten Funktionsübertragung oder Auftragsdatenverarbeitung erfolgen (vgl. Abschnitt 6.1).

Unabhängig von der Frage der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung ist im Rahmen von IT-Outsourcing-Projekten zu klären, ob die personenbezogenen Daten an Dritte in Gebieten außerhalb des Europäischen Wirtschaftsraums übermittelt werden dürfen. Insoweit gilt ein grundsätzliches Übermittlungsverbot, d.h. die Übermittlung darf nur stattfinden, wenn der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein solches entgegenstehendes schutzwürdiges Interesse ist jedoch regelmäßig dann anzunehmen, wenn bei den empfangenden Stellen ein "angemessenes Datenschutzniveau" nicht gegeben ist. Ob ein solches angemessenes Datenschutzniveau tatsächlich gegeben ist, wird von der EU-Kommission festgestellt. Bislang wurde eine entsprechende Angemessenheitsentscheidung erst für die Länder Argentinien, Guernsey, Isle of Man, Kanada und Schweiz getroffen (vgl. dazu Abschnitt 6.2.).

3.3.6 Sarbanes-Oxley-Act – Vorschriften für Kontrollsysteme

Der Sarbanes-Oxley-Act (SOX) wurde im Jahr 2002 in den USA verabschiedet. Die Vorschriften des SOX gelten für alle Unternehmen, die gemäß dem Securities Act von 1934 bei der US-amerikanischen SEC registriert sind und an diese berichten. Dazu gehören auch deutsche Unternehmen.

Ziel dieses Gesetzes ist es, das verlorene Vertrauen der Kapitalmärkte in publizierte Finanzdaten wiederherzustellen. Die Forderung nach der Installation eines effektiven internen Kontroll-Systems durch CEO und CFO sowie die Verpflichtung zu einer regelmäßigen Überprüfung der Wirksamkeit der wichtigsten Kontrollen sind das Kernstück dieser Bestrebungen. Für die Beschreibung eines notwendigen internen Kontroll-Systems spielt vor allem der Abschnitt 404 („Section 404“) des Gesetzes eine Rolle. Dort wird die Installation sowie die jährliche Überprüfung und Bewertung eines internen Kontroll-Systems für das Finanzberichtswesen durch CEO und CFO gefordert. Des Weiteren erfordert „Section 404“ die Bestätigung der Bewertung des CEO und CFO durch einen unabhängigen Wirtschaftsprüfer.

Im Zuge von ausgelagerten Geschäftsprozessen, hauptsächlich in Bezug auf die Finanzbuchhaltung und damit im Zusammenhang stehenden IT-Anwendungen, werden im Auftrag von Unternehmen, die an einer US-Börse notiert sind, verstärkt auch deutsche Tochtergesellschaften und deren Outsourcing-Dienstleister auf Einhaltung der SOX-Anforderungen geprüft. Ähnliche Anforderungen an die Unternehmenskontrolle werden inzwischen auch auf EU-Ebene diskutiert. Die Einführung SOX-ähnlicher Anforderungen über die EU oder über nationale Gesetzgebungsorgane ist also auch für deutsche, börsennotierte Unternehmen bald zu erwarten.

3.4 Richtlinien, Grundsätze und Rundschreiben

3.4.1 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

Richtlinien, Grundsätze und Rundschreiben haben keinen Gesetzes-Charakter. Auf sie wird jedoch in Gesetzestexten oft verwiesen. In einigen Fällen haben Richtlinien einen verbindlichen Charakter für eine besondere Zielgruppe²¹. Alle hier genannten Richtlinien, Grundsätze und Rundschreiben stehen im Zusammenhang mit dem Risiko-Management der Unternehmensleitung und insbesondere mit der Sicherheit der IT – dabei ist es gleichgültig, ob die IT selbst oder von einem Dritten betrieben wird.

In engem Zusammenhang mit den Grundsätzen ordnungsgemäßer Buchführung stehen die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) genannt, die vor allem in den §§ 146 Abs. 5, 147 Abs. 6 Abgabenordnung (AO) eine rechtliche Grundlage haben und u.a. die Anforderung an Unternehmens-Software definieren, dass die betriebswirtschaftlichen Daten vom Prüfer bzw. der speziellen Prüfungs-Software erfasst werden können. Die GDPdU beinhalten u.a. das Recht und die Art des Zugriffs der Finanzbehörden auf digitale Daten und EDV-Systeme, die im Zusammenhang mit der Besteuerung des Unternehmens bei Betriebsprüfungen verwendet werden.

Nicht nur die an einen Dritten ausgelagerten Buchführungs-Dienstleistungen müssen den Anforderungen der GDPdU entsprechen; auch der IT-Dienstleister, der z.B. lediglich SAP-Systeme zur Finanzbuchhaltung betreibt, muss auf die GDPdU z.B. in Bezug auf die gesetzeskonforme Datenarchivierung und Datenhistorisierung von Daten der Finanzbuchhaltung oder anderer steuerlich relevanter Systeme verpflichtet werden.

3.4.2 Baseler Eigenkapitalvereinbarung

Die Baseler Eigenkapitalvereinbarung von 2004 (Basel II) legt fest, dass Banken u.a. vor jeder Fremdmittelvergabe das Risiko der Gesellschaft per Rating einschätzen müssen. Ein entsprechender Gesetzesentwurf der Bundesregierung liegt vor²² und soll entsprechend den europarechtlichen Vorgaben am 01. Januar 2007 in Kraft treten. Im Rahmen der IT bedeutet dies, dass Kreditunternehmen von Unternehmen, die z.B. ein in ihrer eigenen Einschätzung unzureichendes IT-Risiko-Management betreiben, zusätzliche Sicherheiten oder einen höheren Kreditzins verlangen müssen.

²¹ Beispiel: Basel II für Kredit- und Finanzdienstleistungs-Institute.

²² Abrufbar unter

http://www.bundesfinanzministerium.de/lang_de/DE/Geld_und_Kredit/Aktuelle_Gesetze/Entwurf_eines_Gesetzes_zur_Umsetzung_Bankenrichtlinie_anl,templateld=raw,property=publicationFile.pdf.

Durch die in den Basel II-Richtlinien beschriebenen Anforderungen an Risiko-Management-Systeme der Banken sind Unternehmen in zweifacher Weise betroffen:

- Ein Kreditinstitut muss bei der Kreditvergabe an ein Unternehmen sehr viel genauer auf das jeweilige Ausfallrisiko achten und wird seine eigene Messmethode zur Bestimmung des möglichen Risikos anwenden. Eines der Risikofaktoren für das Kreditinstitut ist u.a. die Möglichkeit des Geschäftsausfalls beim Kreditnehmer. Basiert dieser z.B. seine kritischen Geschäftsprozesse hauptsächlich auf IT-Systeme und sind diese besonders anfällig, sind von Bankenseite Risikovorkehrungen zu treffen²³. Hinzu kommt natürlich die Kontrolle über ausgelagerte geschäftskritische Prozesse.
- Betreibt ein Outsourcing-Anbieter geschäftskritische IT-Prozesse für eine Bank, so muss er sich sehr viel detaillierteren internen Kontrollanforderungen unterwerfen, als das bisher der Fall war. Typischerweise werden dadurch Risikovorkehrungen wie z.B. eine funktionierende Notfallplanung, ein regelmäßiger und kontrollierter Datensicherungs- und -wiederherstellungs-Prozess oder ein detailliertes Zugangsberechtigungs-System zu kritischen Systemen extrem wichtig – um nur einige Beispiele zu nennen.

3.4.3 Rundschreiben und sonstige Bekanntmachungen der BaFin

Insbesondere im Bereich der Kredit- und Finanzdienstleistungsbranche sind Rechtsverordnungen, zahlreiche Rundschreiben und sonstige Bekanntgaben der BaFin zu beachten. Während Rechtsverordnungen zwingend anzuwenden sind, stellen Rundschreiben und sonstige Bekanntmachungen, die in der Regel Rechtsnormen in Einzelfragen interpretieren und Verhaltenspflichten vorschreiben sollen, formal nicht bindendes Recht dar. Angesichts der weitgehenden Befugnisse, die das KWG der BaFin einräumt²⁴, und der Tatsache, dass die BaFin die Institute anhand dieser Maßstäbe misst, entfalten diese Äußerungen der BaFin eine mittelbare Wirkung. Somit besteht regelmäßig ein faktischer Zwang zu deren Umsetzung. Exemplarisch genannt seien:

- Rundschreiben 11/2001 des BAKred (heute BaFin), welches sich ausführlich mit der Frage der Auslagerung von Bereichen auf ein anderes Unternehmen gemäß § 25 Abs. 2 KWG befasst und die dort aufgeführten Anforderungen näher konkretisiert.
- Rundschreiben 18/2005 der BaFin (MaRisk)²⁵, welches auf der Grundlage des § 25a Abs. 1 KWG erlassen wurde und Mindestanforderungen an das Risiko-Management in deutschen Kreditinstituten aufstellt.

²³ Eine solche Vorkehrung wäre z.B. ein erhöhter Zinssatz zur Abdeckung des erhöhten Risikos.

²⁴ vgl. insbesondere §§ 35 ff. KWG.

²⁵ Abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm.

3.5 Normen und Standards

3.5.1 Buchführungs-Standards

Ein Standard ist eine vergleichsweise einheitliche, weithin anerkannte Art und Weise etwas durchzuführen. Im Zuge einer Normung werden Standards von anerkannten Gremien wie DIN oder ISO durch Beteiligung aller interessierten Kreise im Konsens erarbeitet und veröffentlicht.

Im Zusammenhang mit Outsourcing-Projekten kann es hilfreich sein, auf etablierte Normen und Standards in der Durchführung von IT-Prozessen zurückzugreifen. Im Falle der Wirtschaftsprüfung veröffentlicht das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) fachliche Regeln zur Gewährleistung eines einheitlichen und hochwertigen Qualitätsniveaus (vgl. Abschnitt 3.5.2).

Im Rahmen der Buchführung sind die Grundsätze ordnungsgemäßer Buchführung (GoB) und die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)²⁶ zu beachten, die teilweise kodifiziert sind²⁷. Für deren Einhaltung ist alleine der Buchführungspflichtige verantwortlich. Auch wenn eine DV-Buchführung im Auftrag durch Fremdfirmen durchgeführt wird, obliegt die Einhaltung der GoB und GoBS dem auftraggebenden Buchführungspflichtigen.

Vor allem bei der Auslagerung von bestimmten Buchhaltungsaufgaben ist deshalb verstärkt auf die Kontrolle der Einhaltung der GoBS zu achten.

Die Grundsätze ordnungsmäßiger Buchführung bei IT-gestützter Rechnungslegung (GoBS) sind nur erfüllt, wenn das Rechnungslegungs-System die Einhaltung der folgenden allgemeinen Ordnungsmäßigkeits-Kriterien bei der Erfassung, Verarbeitung, Ausgabe und Aufbewahrung der rechnungslegungsrelevanten Daten über die Geschäftsvorfälle sicherstellt:

- Vollständigkeit (§ 239 Abs. 2 HGB)
- Richtigkeit (§ 239 Abs. 2 HGB)
- Zeitgerechtigkeit (§ 239 Abs. 2 HGB)
- Ordnung (§ 239 Abs. 2 HGB)
- Nachvollziehbarkeit (§ 238 Abs. 1 Satz 2 HGB)
- Unveränderlichkeit (§ 239 Abs. 3 HGB).

²⁶ Gemäß Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995 - IV A 8 - S 0316 - 52/95- BStBl. 1995 I S. 738.

²⁷ z.B. in HGB und AO.

3.5.2 Wirtschaftsprüfungs-Standards

Die nachfolgend ausgewählten Wirtschaftsprüfungs-Standards des IDW konkretisieren die aus den §§ 238, 239 und 257 HGB resultierenden Anforderungen an die Führung der Handelsbücher mittels IT-gestützter Systeme und verdeutlicht die beim Einsatz von IT möglichen Risiken für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung. Sie beziehen sich in Teilen auch auf ausgelagerte IT-Prozesse, sofern diese rechnungslegungsrelevant sind.

■ **Buchführungsgrundsätze bei IT-Einsatz (IDW RS FAIT 1):**

Der Fachausschuss für Informationstechnologie (FAIT) des IDW hat mit der Stellungnahme zur Rechnungslegung (RS) FAIT 1 „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ einen für Wirtschaftsprüfer anzuwendenden Prüfungsstandard veröffentlicht. Dieser beschreibt Anforderungen an die Ordnungsmäßigkeit und Sicherheit für IT-gestützte Systeme und steht in engem Zusammenhang mit den GoBS.

Der Einsatz von IT im Unternehmen erfolgt in Form eines IT-Systems, das zur Verarbeitung von Daten folgende Elemente beinhaltet:

- IT-gestützte Geschäftsprozesse
- IT-Anwendungen
- IT-Infrastruktur.

Das Zusammenwirken dieser Elemente wird durch das IT-Kontrollsystem bestimmt, das von dem IT-Umfeld und der IT-Organisation abhängt. Das IT-Kontrollsystem ist Bestandteil des internen Kontrollsystems (IKS). Es umfasst diejenigen Grundsätze, Verfahren und Maßnahmen (Regelungen), die zur Bewältigung der Risiken aus dem Einsatz von IT eingerichtet werden. Hierzu gehören Regelungen zur Steuerung des Einsatzes von IT im Unternehmen (internes Steuerungssystem) und Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem)²⁸.

IT-Kontrollen sind Bestandteil des internen Überwachungssystems. Zu ihnen zählen die in IT-Anwendungen enthaltenen Eingabe-, Verarbeitungs- und Ausgabekontrollen sowie alle im IT-System vorgesehenen prozessintegrierten Kontrollen und organisatorischen Sicherungsmaßnahmen wie z.B. Zugriffskontrollen oder Netzwerkkontrollen auf der Ebene der IT-Infrastruktur. Darüber hinaus gehören zu den IT-Kontrollen auch solche Maßnahmen, die sich unabhängig von der jeweiligen IT-Anwendung als generelle Kontrollen auf das gesamte IT-System auswirken²⁹.

²⁸ Vgl. IDW Prüfungsstandard: Das interne Kontrollsystem im Rahmen der Abschlussprüfung (IDW PS 260), Tz. 5, 6; in: WPg 2001, S. 821 ff.

²⁹ z.B. Kontrollen der Entwicklung, Einführung und Änderung von IT-Anwendungen (Change-Management).

FAIT 1 widmet u.a. einen kompletten Abschnitt (4.6.) dem IT-Outsourcing. Darin heißt es, dass die Unternehmensleitung die Auswirkungen auf das interne Kontrollsystem des Unternehmens beachten müssen, sollten die betrieblichen Funktionen (einschließlich IT-gestützter Funktionen) auf ein anderes Unternehmen ausgelagert werden. Sofern im Rahmen des Outsourcings die Ausführung von Geschäftsvorfällen oder die Datenverarbeitung von einem damit beauftragten Dienstleistungs-Unternehmen wahrgenommen werden, verbleibt die Verantwortung für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen bei den gesetzlichen Vertretern des Unternehmens.

■ **Abschlussprüfung bei IT-Einsatz (IDW PS 330):**

Der IDW Prüfungs-Standard 330 stellt einen Leitfaden für die Wirtschaftsprüfer zur „Abschlussprüfung bei Einsatz von Informationstechnologie“ dar. Der Abschlussprüfer muss im Rahmen seiner Abschlussprüfung auch IT-gestützte Rechnungslegungs-Systeme hinsichtlich der gesetzlichen Vorschriften zur Ordnungsmäßigkeit und Sicherheit prüfen. Die IT-Systemprüfung zielt auf die Bewertung von Risiken für erhebliche Fehler im IT-System, solange diese die Rechnungslegung beeinflussen.

In Abschnitt 3.8 des IDW PS 330 wird explizit auf das IT-Outsourcing eingegangen. Der Abschlussprüfer muss beurteilen, wie sich eine ausgelagerte IT-Komponente auf das interne Kontroll-System des Unternehmens auswirkt. In diesem Zusammenhang sind für die Abschlussprüfung auch die im Dienstleistungs-Unternehmen eingerichteten organisatorischen Regelungen und die vorgehaltenen Aufzeichnungen zu bewerten. Falls der Abschlussprüfer während seiner Prüfung die Auswirkung eines Outsourcing-Dienstleisters auf den Kunden als wesentlich einstuft, so müssen zur Risikoeinschätzung auch das Kontroll-System des Outsourcing-Dienstleisters und weitere Informationen überprüft werden. Tangiert das IT-Outsourcing die Buchführung, so muss zuallererst die Ordnungsmäßigkeit des Service-Unternehmens geprüft werden. Diese Beurteilung kann auch durch Prüfungsergebnisse eines Abschlussprüfers des Dienstleisters oder Sachverständige ergänzt werden.

3.5.3 Prüfungs- oder Implementierungs-Standards für die Zertifizierung von IT-Prozessen

Die Anforderungen an die Einführung von Kontroll-Systemen bzw. Risiko-Management-Systemen haben in der Vergangenheit immer mehr zugenommen. Insbesondere haben gesetzliche Vorgaben wie das KonTraG oder SOX den Druck für die IT-Organisation der Unternehmen verschärft, ein internes Kontroll-System einzuführen. Ein Anbieter von IT-Outsourcing ist hiervon natürlich besonders betroffen, da er unterschiedliche Anforderungen an interne Kontroll-Systeme von seinen Kunden erhält. Um die Einführung und Ausgestaltung IT-spezifischer Kontroll-Systeme für solche

Unternehmen zu erleichtern, lohnt ein Blick auf verschiedene Standards, die auch eine Zertifizierung der definierten Kontroll-Systeme und -prozesse ermöglichen³⁰ (vgl. Tabelle 4)

Tabelle 4: Standards mit Möglichkeit zur Zertifizierung von Kontroll-Systemen

Standard	Erläuterung
SAS 70	<p>Der Vorteil einer Bestätigung nach dem Statement on Auditing Standards (SAS) No. 70 des American Institute of Certified Public Accountants (AICPA) besteht darin, dass einzelne interne Kontrollen oder das gesamte interne Kontroll-System eines Unternehmens einer detaillierten Prüfung durch den Wirtschaftsprüfer unterzogen und die Ergebnisse in einem standardisierten Bericht nach Typ I oder II dokumentiert werden können. Eine Bestätigung des internen Kontroll-Systems nach SAS 70 Typ I gibt dabei „nur“ eine Aussage über das Design des internen Kontroll-Systems, während ein SAS 70 Typ II Bericht die Wirksamkeit der internen Kontrollen oder des gesamten internen Kontroll-Systems bestätigt.</p> <p>Der SAS 70 Typ II Bericht (vgl. Tabelle 5) kann den Aufwand für mehrere Prüfungen durch Abschlussprüfer, Revisoren oder andere unabhängige Prüfer seitens der Outsourcing-Kunden reduzieren helfen.</p> <p>Für das IT-Outsourcing Geschäft wird eine Zertifizierung nach SAS 70 immer wichtiger. Zunächst hauptsächlich getrieben durch die SOX-Anforderungen, hat sich SAS 70 als „Quasi“-Standard für die Zertifizierung interner IT-Kontroll-Systeme ausgelagerter IT-Dienstleistungen³¹ etablieren können. Die Nutzung und Akzeptanz eines SAS 70 Reports hängt aber immer an der Entscheidung des betroffenen Wirtschaftsprüfers. Deshalb sollten Aktivitäten in diese Richtung immer im Vorfeld mit allen beteiligten Wirtschaftsprüfern abgestimmt werden.</p>
IDW PS 331	<p>Der IDW Prüfungs-Standard 331 „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungs-Unternehmen“ geht spezifisch auf die schon im Wirtschaftsprüfungsstandard IDW PS 330 genannten Anforderungen, die an die IT-Landschaft eines Unternehmens gestellt werden ein, bezieht sich jedoch explizit auf die von einem Unternehmen ausgelagerten IT-bezogenen Rechnungslegungs-Dienstleistungen.</p>

³⁰ Ob der Wirtschaftsprüfer vorgelegte Zertifizierungen nutzt, muss individuell abgesprochen werden. Eine Zertifizierung kann dabei eine Prüfung niemals komplett ersetzen, sondern bestenfalls den Aufwand für einzelne Prüfungsmaßnahmen vermindern.

³¹ bzw. auch anderer Dienstleistungen wie Gehaltsabrechnungs-Dienstleistungen.

Standard	Erläuterung
	<p>Der Abschlussprüfer eines Unternehmens muss sich auch vom ordnungsgemäßen Betrieb der ausgelagerten Rechnungslegungs-Dienstleistungen im Rahmen der Abschlussprüfung überzeugen. So sind die ausgelagerten, zumeist IT-bezogenen Rechnungslegungs-Dienstleistungen direkt bei dem Outsourcing-Anbieter zu prüfen. Der Abschlussprüfer kann aber unter Beachtung gesonderter Regelungen bei der Verwendung der Arbeit eines anderen externen Prüfers entscheiden, ob er möglicherweise die Vorlage einer Zertifizierung nach IDW PS 331 des Outsourcing-Anbieters für seine eigene Prüfung nutzt. Insofern könnte man eine Zertifizierung nach dem Prüfungs-Standard IDW PS 331 als „deutsche Variante des SAS 70 Reports“ verstehen. Allerdings hat sich für diese Zwecke der SAS 70 Report vor allem auch im internationalen Umfeld wesentlich stärker etablieren können.</p> <p>Die Prüfungs-Standards IDW PS 331 und SAS 70 enthalten lediglich Vorgaben, wie der Wirtschaftsprüfer bestimmte Prozesse zu prüfen hat. Die eigentlichen Inhalte der Prüfung sind jedoch individuell festzulegen. Das Outsourcing-Unternehmen muss demnach selbst festschreiben, welche Prozesse zu prüfen und zu zertifizieren sind. Es wird empfohlen, sich bei den genauen Inhalten mit den betroffenen Kunden und deren Abschlussprüfern abzustimmen.</p>
BSI-Grundschutz	<p>Das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) enthält Empfehlungen und Hilfsmittel für die Umsetzung der IT-Sicherheit in der öffentlichen Verwaltung und in privatwirtschaftlichen Unternehmen. Der IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen, um damit ein angemessenes Sicherheitsniveau zu erreichen. Zur Einführung eines entsprechenden IT-Sicherheitsniveaus gehören inzwischen auch Sicherheitszertifizierungen nach ISO-Standards (vgl. Abschnitt 3.5.4) auf Basis von IT-Grundschutz, die sowohl eine Prüfung des IT-Sicherheits-Managements als auch der konkreten IT-Sicherheitsmaßnahmen umfasst. Verpflichtend vorgeschrieben ist der BSI-Grundschutz in vielen Bereichen der öffentlichen Verwaltung.</p> <p>Eine Zertifizierung nach BSI-Grundschutz kann einem Outsourcing-Dienstleister gegenüber seinen Kunden helfen, eine gutes Grundniveau für bestehende Sicherheitsmaßnahmen von einem externen Dritten bestätigen zu lassen. Eine BSI-Grundschutz-Zertifizierung kann aber die Arbeit eines Wirtschaftsprüfers in Bezug auf Bestätigungsvermerke zur Ordnungsmäßigkeit eingesetzter Kontrollsysteme nicht ersetzen oder ergänzen.</p>

Standard	Erläuterung
ISO 17799	<p>Der ISO 17799 Standard wurde 1995 als BS 7799 das erste Mal herausgegeben, um eine umfassende Sammlung von Maßnahmen bereitzustellen, in der die besten Praktiken in der Informations-Sicherheit enthalten sind. Dieser Standard sollte gemeinsamer Bezugspunkt zur Identifizierung der verschiedenen Maßnahmen sein, die für die meisten Situationen erforderlich sind, in denen Informationssysteme in Industrie und Handel verwendet werden. Deshalb sollte der Standard in Organisationen aller Größenklassen zum Einsatz kommen.</p> <p>Bis heute hat der Sicherheitsstandard einige wichtige Aktualisierungen erfahren und wird zukünftig unter der ISO Standard Serie 27000³² geführt werden.</p> <p>Informations-Sicherheit wird hier verstanden als Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen oder Daten. Sie sollte der Grundpfeiler eines effektiven Risiko-Management-Systems aller Unternehmen sein.</p> <p>Im Zusammenhang mit ausgelagerten Dienstleistungen, vor allem z.B. im Bereich IT-Outsourcing, gewinnt der Sicherheits-Standard ISO 17799 (bzw. ISO 27001) eine immer größere Bedeutung. Eine Zertifizierung nach ISO 27001 durch eine unabhängige Stelle ist für Outsourcing-Anbieter möglich und als wichtiger Bestandteil eines strukturierten internen Kontroll-Systems zur Erfüllung von Compliance-Anforderungen auch sinnvoll. Die Zertifizierung nach ISO 27001 kann aber die Prüfung interner Kontrollen z.B. durch den Wirtschaftsprüfer nicht ersetzen.³³</p>

³² je nach Themengebiet 27001-27004.

³³ Das „Fallbeispiel 1 - IT-Sicherheit“ (vgl. Abschnitt 7.2) geht im Detail auf Standards für die Informations-Sicherheit ein und erläutert die praktische Umsetzung.

Tabelle 5: SAS 70 Berichte im Überblick

SAS 70 Typ	Erläuterung
I "Report on controls placed in operation"	Die im Service-Unternehmen vorgesehenen internen Kontrollen, die in der Beziehung zu seinen Kunden und deren Prüfung des Jahresabschlusses relevant sind, werden auf Ihre Angemessenheit und Anwendung hin überprüft. Der Report Typ I umfasst die Beschreibung und die Anwendung des Internen Kontroll-Systems, aber nicht den Test der eingesetzten Kontrollmaßnahmen.
II ³⁴ "Report on controls placed in operation and test of operating effectiveness"	Dieser Report umfasst zusätzlich zu den Analysen des Reports Typ I die Überprüfung der Kontrollen im Hinblick auf ihre Effizienz und Wirksamkeit bei deren Umsetzung. Er bietet dadurch wichtige Informationen für Kunden des Service-Unternehmens, die eine Aussage über die abgedeckten Kontrollen erhalten und somit deren eigene interne Kontrollen entsprechend optimieren können.

3.5.4 DIN-, ISO-, IEC-Normen und Best Practice

Weiterhin existieren zahlreiche DIN-, ISO-, IEC-Normen und „Best Practice“, welche einen Maßstab für einwandfreies Verhalten bilden und zumindest mittelbar verbindlich werden können. Hierbei ist zu beachten, dass für die mittelbare Geltung eine ausdrückliche Bezugnahme durch Gesetze oder Verordnungen nicht zwingend ist. Vielmehr wird beispielsweise bei der Frage, ob ein Schaden schuldhaft³⁵ verursacht wurde, häufig auf anerkannte Standards zurückgegriffen³⁶. Sofern ein anerkannter Standard eingehalten wurde, lassen sich in der Regel gute Argumente dafür finden, dass die im Verkehr erforderliche Sorgfalt beachtet wurde.

Exemplarisch zu nennen sind die:

- Normenreihe EN ISO 9000 ff., welche Grundsätze für Maßnahmen zum Qualitäts-Management dokumentiert,
- Normen ISO/IEC 9126, welche ein Modell zur Sicherstellung/Messung von Softwarequalität darstellen,

³⁴ Ein typischer SAS 70 Typ II Reports besteht aus 4 Teile: Teil 1: Bestätigungsvermerk des Wirtschaftsprüfers, Teil 2: Beschreibung der internen Kontrollen und Kontrollziele, Teil 3: Prüfungshandlungen: Test der operativen Wirksamkeit, Ergebnisse der Tests, Teil 4: Zusatzinformationen (optional), werden vom Wirtschaftsprüfer nicht bewertet.

³⁵ Schuldhaft bedeutet vorsätzliche oder fahrlässige Verursachung. Fahrlässigkeit heißt, dass die im Verkehr erforderliche Sorgfalt nicht eingehalten wurde.

³⁶ Zur Ausfüllung des Sorgfaltsmaßstabs durch a) DIN-Normen siehe z. B. BGHZ 103, S. 341; BGHZ 139, S. 17, b) technische Regeln siehe z. B. BGHZ 54, S. 335, c) durch Richtlinien des Spitzenverbandes der Banken siehe NJW 1990, S. 2262.

- Normen ISO/IEC 27001, welche die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informations-Sicherheits-Management-Systems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation spezifizieren.

Der ISO 9001:2000 befasst sich mit den Anforderungen von Qualitäts-Management-Systemen. Als Voraussetzung für eine funktionierende Organisation nennt der Standard die Identifizierung, Leitung und Lenkung von verknüpften Tätigkeiten. Je besser das Zusammenspiel der verknüpften Tätigkeiten ist, desto hochwertiger ist das Ergebnis. Weiterhin wird für dieses Ziel ein prozessorientierter Ansatz gefördert und empfohlen. Für Unternehmen besteht die Möglichkeit, sich nach diesem internationalen Standard zertifizieren zu lassen.

Zahlreiche Outsourcing-Anbieter und andere Dienstleister haben ihre Qualitäts-Management-Systeme nach ISO 9001:2000 zertifizieren lassen. Generell sollte aber bei allen Zertifizierungsbemühungen immer daran gedacht werden, wer die genaue Zielgruppe der Zertifizierungsbotschaft ist. Zur Verwendung in Marketingbotschaften kann die ISO 9001:2000 wichtig sein, solange der jeweilige Kunde diese Zertifizierung vom Dienstleistungs-Anbieter verlangt. In den letzten Jahren haben sich aber noch einige andere Aufgabenfelder für eine Standardisierung im Outsourcing-Umfeld herauskristallisiert³⁷.

3.6 Referenzmodelle

Ein Referenzmodell stellt ein allgemeines Modell für eine Klasse von Sachverhalten mit folgenden Eigenschaften dar:

- Auf Basis des allgemeinen Modells können spezielle Modelle (als Grundlage für die Konstruktion ganz bestimmter Sachverhalte) geplant werden.
- Das allgemeine Modell kann als Vergleichsobjekt herangezogen werden, d.h. es ermöglicht Vergleiche mit anderen Modellen, die die gleichen Sachverhalte beschreiben.

Das Referenzmodell bildet somit ein Modellmuster, das als idealtypisches Modell für die Klasse der zu modellierenden Sachverhalte betrachtet werden kann.³⁸

Im Kontext des vorliegenden Leitfadens dienen Referenzmodelle einer besseren Effizienz bei der Einführung von IT-Kontrollmaßnahmen in Unternehmen (vgl. Tabelle 6). In der Regel sind Referenzmodelle wie CoBIT oder ITIL an Gesetze, Richtlinien oder Standards angelehnt und versuchen den Brückenschlag über eine Vielzahl solcher Regelungen (vgl. S. 22).

³⁷ vgl. dazu SAS 70 und ISO 17799 in Tabelle 4 oder ITIL in Abschnitt 3.6.

³⁸ Zitiert nach: <http://de.wikipedia.org/wiki/Referenzmodell>, 19. Juli 2006.

Tabelle 6: Referenzmodelle

Modell	Erläuterung
COSO	<p>Das COSO-Modell ist ein von der gleichnamigen Organisation (Committee of Sponsoring Organizations of the Treadway Commission) entwickeltes Rahmenwerk für interne Kontroll-Systeme und beschreibt</p> <ul style="list-style-type: none"> ■ eine Methodik für die Einführung der wichtigsten Komponenten eines internen Kontroll-Systems wie z.B. das Kontrollumfeld im Unternehmen, ■ das Vorgehen bei der Risikobeurteilung, ■ die konkret einzuführenden Kontrollaktivitäten, ■ Maßnahmen der Information und Kommunikation im Unternehmen und ■ notwendige Maßnahmen der Überwachung des Kontroll-Systems. <p>Das COSO-Modell geht zunächst nicht spezifisch auf IT-Abläufe und IT-Outsourcing ein, sondern stellt die Grundstruktur für ein allgemein einzuführendes internes Unternehmens-Kontroll-System dar. Es gilt als Basis für Referenzmodelle wie CoBIT und erleichtert dessen Einführung.</p>
CoBIT	<p>Die ISACF (Information Systems Audit Control Foundation) hat 1996 das Referenzmodell CoBIT (Control Objectives for Information and Related Technology) entwickelt und mehrfach weiterentwickelt. Der Grundgedanke hinter dem CoBIT-Modell ist es, ein generell anwendbares und international akzeptiertes Rahmenwerk zur Verfügung zu stellen, welches die in einem IT-Kontroll-System zu erfüllenden Kontrollziele im Detail definiert. Diese sogenannten CoBIT Control Objectives haben einen direkten Bezug zu den im COSO-Modell definierten Schichten eines allgemeinen internen Kontroll-Systems. Zu beachten ist, dass die im Rahmen von CoBIT definierten Kontrollziele zwar vorschlagen, was als Bestandteil eines internen IT-Kontroll-Systems zu prüfen ist, jedoch keine Angaben enthalten, wie die entsprechenden Prüfungen der definierten Kontrollziele durchzuführen sind.</p> <p>Es wird empfohlen, dass beide Partner in einem Outsourcing-Deal CoBIT für die Einführung eines internen Kontroll-Systems für die ausgelagerten IT-Dienstleistungen nutzen. Wirtschaftsprüfer haben an der Entwicklung des CoBIT-Referenzmodells mitgewirkt, und man findet in den meisten Prüfungspläne die CoBIT-Kontrollziele wieder. Sie decken die wesentlichen IT-Prozesse und die darin enthaltenen und notwendigen Kontrollen ab. Selbst bei der Definition prüfungsrelevanter Aspekte im SLA mit dem Outsourcing-Anbieter könnte bei Bedarf auf einzelne Kontrollziele von CoBIT verwiesen werden. Inhalte und Umfang der in einem SLA aufzunehmenden Kontrollen sollten im Vorfeld gemeinsam mit dem eigenen Abschlussprüfer abgestimmt werden.</p>

Modell	Erläuterung
ITIL	<p>ITIL ist der meist verbreitete Best-Practice-Ansatz für das IT-Service-Management. ITIL geht von der Überlegung aus, dass die Information als strategisch wichtigste Ressource in einer Organisation im Fokus des Managements stehen sollte. Die IT muss möglichst gut mit der Unternehmensstrategie und den Geschäftsprozessen abgestimmt sein und darf nicht isoliert betrachtet werden. Einen wesentlichen Beitrag zur Zielerreichung leistet ein reibungsloses und effektives „Betreiben“ von Prozessen.</p> <p>Dafür werden in ITIL verschiedene „Best Practice“ Prozesse für die Bereiche Service Support, Service Delivery, Kommunikationstechnologien, Infrastruktur Management, Applikationsmanagement und Sicherheits-Management genannt.</p> <p>Die Arbeit mit ITIL ist für das IT-Outsourcing von hoher Bedeutung, da so Wissen über die Kundenprozesse entsteht und daher ein Service besser und qualitativ hochwertiger erbracht werden kann. Weiterhin kann durch ITIL auch eine höhere Stabilität der IT gewährleistet werden, da die „Best Practice“-Prozesse alle Elemente des IT-Betriebs in detaillierter Form nennen, von denen vielleicht vorher einige kritische Prozesse außer Acht gelassen wurden.</p> <p>Zu beachten ist jedoch, dass die Einführung und Zertifizierung des ITIL-Modells im Unternehmen nicht automatisch die Erfüllung der Compliance-Anforderungen nach SOX oder der Anforderungen an prüfungsrelevante Kontroll-Systeme nach sich zieht. ITIL bietet dem Outsourcing-Anbieter eine gute Basis für eine strukturierte IT-Organisation und bringt ihn demzufolge einen wichtigen Schritt in Richtung Compliance. Die Anforderungen an ein internes IT-Kontroll-System sind aber separat zu betrachten und werden allein durch die Einführung von ITIL nicht abgedeckt werden können.</p>

4 Risiken der Nichteinhaltung und vertragliche Abbildung rechtlicher Rahmenbedingungen

Merksatz 3

Die bei einem Outsourcing-Projekt zu beachtenden rechtlichen Anforderungen sind vom Gesetzgeber in Deutschland und anderen Ländern deutlich verschärft worden. Hierdurch hat sich zugleich das persönliche zivilrechtliche sowie strafrechtliche Haftungsrisiko von Führungskräften nachhaltig erhöht. Daran ändert Outsourcing praktisch nichts. Um dieser Verantwortung nachzukommen, bedarf es vertraglicher Bestimmungen, die die Verantwortung für die Einhaltung bestimmter rechtlicher Rahmenbedingungen sowie die Steuerungs- und Kontrollrechte des auslagernden Unternehmens regeln.

4.1 Überblick

Die bei einem Outsourcing-Projekt zu beachtenden rechtlichen Rahmenbedingungen sind vom Gesetzgeber in Deutschland und anderen Ländern - angesichts spektakulärer Firmenzusammenbrüche in der Vergangenheit³⁹ - deutlich verschärft worden. Hierdurch hat sich zugleich das persönliche zivilrechtliche sowie strafrechtliche Haftungsrisiko von Führungskräften nachhaltig erhöht. Auch wenn die technische Durchführung entsprechender Aufgaben an einen externen Dienstleister ausgelagert wird, so bleibt das Management eines Unternehmens weiterhin in vollem Umfang für die Erfüllung dieser Anforderungen (vgl. Kapitel 3) verantwortlich. Um dieser Verantwortung nachzukommen, bedarf es insbesondere vertraglicher Bestimmungen, die

- zum einen die Verantwortung für die Einhaltung bestimmter rechtlicher Rahmenbedingungen,
- zum anderen aber auch die Steuerungs- und Kontrollrechte des auslagernden Unternehmens regeln.

Das Kapitel 4

- vermittelt in einem ersten Schritt einen Überblick über die zivil- wie strafrechtlichen Verantwortlichkeiten des Unternehmens-Managements im Zusammenhang mit der Einhaltung rechtlicher Rahmenbedingungen und
- gibt in einem zweiten Schritt in Form von Klauselbeispielen Anregungen für einzelne vertragliche Regelungen.

³⁹ Z.B. Schneider und Balsam in Deutschland sowie Enron und Worldcom in den USA.

4.2 Sanktionen und Haftungsrisiken

4.2.1 Allgemeines

Eine fehlende oder mangelhafte Einhaltung rechtlicher Rahmenbedingungen kann zu einer privatrechtlichen Haftung des Unternehmens und der Organe des Unternehmens gegenüber der Gesellschaft sowie gegenüber anderen Dritten und einer Haftung nach Ordnungswidrigkeiten- und Strafrecht führen. Im zivilrechtlichen Bereich kommen dabei insbesondere Beseitigungs-, Auskunfts-, Unterlassungs- und Schadenersatzansprüche in Betracht. Auch eine persönliche Haftung des Geschäftsleitungsmitglieds gegenüber Dritten kommt dabei in Betracht, dürfte allerdings eher die Ausnahme bleiben, da hierfür die Verletzung eines deliktisch geschützten Rechts-guts⁴⁰ oder eines Schutzgesetzes⁴¹ notwendig ist. Daneben besteht auch die Möglichkeit einer Haftung von sonstigen Führungskräften wie z.B. IT-Verantwortlicher, Datenschutzbeauftragter und Fachbereichsleiter, auf die in diesem Leitfaden nicht näher eingegangen wird. In ordnungswidrigkeitenrechtlicher Hinsicht drohen Untersagungsverfügungen und Bußgelder, im Strafrecht Geld- und Freiheitsstrafen⁴².

Die Sanktionen und Haftungsrisiken für die Nichteinhaltung rechtlicher Rahmenbedingungen sind so vielfältig, dass eine umfassende Darstellung hier nicht möglich ist⁴³. Geschildert seien hier aufgrund besonderer Relevanz für das IT-Outsourcing lediglich einige Sanktionen, die auf Verstößen gegen Datenschutz- und Bankaufsichtsrecht beruhen. Darüber hinaus sei auf die relevantesten strafrechtlichen Bestimmungen hingewiesen:

- Bei Verstößen gegen das BDSG stehen zunächst dem betroffenen Datensubjekt gemäß §§ 6, 7, 34 und 35 BDSG Auskunfts-, Berichtigungs-, Sperrungs-, Löschungs-, Unterlassungs- und Schadenersatzansprüche zu. Schwere Verstöße können (verwaltungsrechtlich) gemäß § 43 Abs. 3 BDSG Bußgelder von bis zu EUR 250.000 und (strafrechtlich) gemäß § 44 Abs. 2 eine Geldstrafe oder Freiheitsstrafe von bis zu 2 Jahren nach sich ziehen.⁴⁴ Zwar sind bisher kaum Fälle bekannt geworden, in denen wegen der Verletzung datenschutzrechtlicher Bestimmungen ein Bußgeld oder gar eine Strafe verhängt wurde, jedoch ist wegen der allgemein zunehmenden Bedeutung des Datenschutzes damit zu rechnen, dass die Behörden in Zukunft die Gesetzesbefolgung strenger überwachen (§ 38 BDSG).

⁴⁰ z.B. Urheberrechtsverletzung durch illegales Kopieren von Software.

⁴¹ Gesetz, das den Schutz eines anderen bezweckt z.B. Geräte- und Produktsicherheitsgesetz (GPSG).

⁴² Die persönliche Verantwortlichkeit des Geschäftsleiters kommt in diesem Zusammenhang über § 14 StGB in Betracht.

⁴³ Vgl. hierzu auch BITKOM Leitfaden Matrix der Haftungsrisiken, abzurufen unter

http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Matrix_der_Haftungsrisiken-V1.1f.pdf.

⁴⁴ wobei die Strafbarkeit nach § 44 BDSG vorsätzliches Handeln gegen Entgelt oder die Absicht voraussetzt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Ferner muss der Betroffene gemäß § 44 Abs. 2 BDSG Strafantrag gestellt haben.

- Beachten die Parteien im Rahmen eines Outsourcing-Projektes im Bankensektor nicht die Regelungen gemäß § 25 a Abs. 2 KWG in Verbindung mit dem Auslagerungsroundschreiben 11/2001, kann die BaFin gemäß § 6 Abs. 3 S. 1 KWG Nachbesserung der Verträge verlangen oder sogar die Auslagerung ganz untersagen. Die BaFin könnte darüber hinaus gemäß § 35 Abs. 2 Nr. 6 KWG auch die Bankenerlaubnis aufheben oder gemäß § 36 Abs. 1, 2 KWG Geschäftsführer abberufen. Zu beachten ist ferner die Möglichkeit, Bußgelder⁴⁵ gemäß § 56 Abs. 2 Nr. 4 KWG wegen unterlassener, verspäteter, unrichtiger oder unvollständiger Anzeigen im Zusammenhang mit dem Auslagerungsvorhaben zu verhängen. Die Nichtbeachtung des § 25 a Abs. 2 KWG führt im übrigen regelmäßig dazu, dass der Abschlussprüfer den uneingeschränkten Bestätigungsvermerk für den Jahresabschluss gemäß § 322 HGB verweigert, was für Unternehmen angesichts drohender Bußgelder gemäß § 334 HGB, eines eventuellen Imageschadens, insbesondere im Verhältnis zu Aktionären und Gläubigern, und nachteiliger Auswirkungen bei der Entlastung von Vorstand und Aufsichtsrat gemäß § 120 AktG eine besonders empfindliche Sanktion ist.
- Die wesentlichen strafrechtlichen Bestimmungen, die es insbesondere im Zusammenhang mit der Auslagerung der IT zu beachten gilt sind: § 202 StGB (Verletzung des Briefgeheimnisses); § 202a StGB (Ausspähen von Daten); § 203 StGB (Verletzung von Privatgeheimnissen)⁴⁶; § 206 (Verletzung des Post- oder Fernmeldegeheimnisses); § 266 (Untreue); § 303a StGB (Datenveränderung); § 303b (Computersabotage).

4.2.2 Spezielle Verantwortung der Geschäftsleitung

Kommt der Vorstand oder Geschäftsführer eines Unternehmens seinen Pflichten nicht nach, sorgt er beispielsweise nicht in ausreichendem Maße für die Einhaltung der für das Unternehmen anwendbaren rechtlichen Rahmenbedingungen⁴⁷ vor, so kann ihn wegen Nichtanwendung der erforderlichen Sorgfalt (vgl. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG) eine persönliche Haftung auf Schadensersatz gegenüber der Gesellschaft gemäß den § 93 Abs. 2 AktG, § 43 Abs. 2 GmbHG treffen.⁴⁸

Diese Haftungsregelung wird noch dadurch verschärft, dass die Geschäftsleitung im Zweifelsfall beweisen muss, dass sie die erforderliche Sorgfalt angewandt hat. Ein solcher Beweis kann im Hinblick auf Aspekte der IT-Sicherheit dann gelingen, wenn die Unternehmensleitung im Rahmen

⁴⁵ Bis EUR 50.000, § 56 Abs. 4 KWG.

⁴⁶ Diese Vorschrift ist wegen § 203 I Nr. 6 insbesondere bei der IT-Auslagerung im Bereich von Kranken-, Unfall- sowie Lebensversicherungen problematisch.

⁴⁷ z.B. durch die Einrichtung eines adäquaten, an internationalen Normen und gesetzlichen Vorgaben orientierten Risiko-Managements.

⁴⁸ Folglich etabliert sich beispielsweise eine Rechtspflicht zur Einrichtung eines (angemessenen) Risiko-Management-Systems immer mehr zu einem Grundsatz ordnungsgemäßer Geschäftsführung.

des Risiko-Managements durch organisatorische und technische Maßnahmen die Risiken im Zusammenhang mit der IT-Sicherheit so weit wie möglich vermindert hat.

Angesichts der Pflicht des Aufsichtsrats zur Verfolgung von Schadensersatzansprüchen gegen Vorstandsmitglieder gemäß den §§ 93 Abs. 2, 111 Abs. 1, 112 AktG, wenn die Ansprüche nach sachgerechter Prüfung Erfolg versprechend erscheinen⁴⁹, und die durch das Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) in § 148 AktG eingeführte Möglichkeit der Aktionärsklage ist das Risiko einer tatsächlichen Inanspruchnahme erheblich gestiegen. Dringen beispielsweise aufgrund unzureichenden Information-Lifecycle-Managements interne Informationen ungewollt an die Öffentlichkeit⁵⁰ oder gehen wichtige Informationen verloren, kann dies haftungsrechtlich auf die Geschäftsleitung durchschlagen, wenn dieser ein Mangel an Sorgfalt vorzuwerfen ist.

4.2.3 Aufsichtsrat

Eine entsprechende Haftung der Mitglieder des Aufsichtsrates gegenüber der Gesellschaft kann sich aus § 116 AktG i.V.m. § 93 Abs. 2 AktG ergeben, wenn diese ihre Überwachungspflicht nicht mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters wahrnehmen. Auch hier ist das Risiko einer tatsächlichen Inanspruchnahme durch die neu eingeführte Möglichkeit der Aktionärsklage (§ 148 AktG) erheblich angestiegen.

Die strafrechtliche Verantwortlichkeit der Aufsichtsratsmitglieder kommt grundsätzlich ebenso in Betracht wie bei Vorstandsmitgliedern, dürfte jedoch aufgrund anderer Funktion und eingeschränkter Vertretungsbefugnisse seltener vorkommen.

4.2.4 Absicherung durch Directors & Officers Versicherung

Eine Absicherung gegenüber derartigen Haftungsrisiken – z.B. über eine D & O-Versicherung – ist demgegenüber nur in engen Grenzen möglich, da der Versicherungsschutz je nach Anbieter und Risikosituation in der Regel durch diverse Ausschlussstatbestände und verhüllte Obliegenheiten zum Teil erheblich begrenzt ist.

⁴⁹ Vgl. BGH, Urt. v. 21.04.1997 („ARAG/Garmenbeck“) in ZIP 1997, 883.

⁵⁰ Vgl. den Fall des US-Investmentbankers Frank Quattrone, der seine Mitarbeiter per E-Mail angewiesen haben soll, verdächtige E-Mails zu löschen und sodann zunächst wegen Justizbehinderung verurteilt, mittlerweile vorerst entlastet wurde; vgl. auch den BITKOM Leitfaden zum sicheren Datenlöschen, abrufbar unter http://www.bitkom.org/files/documents/Leitfaden_Sicheres_Datenloeschen_final_11-10-2004.pdf.

4.3 Aspekte der Vertragsgestaltung⁵¹

Wie bereits deutlich geworden ist, kommt der Beachtung und Einhaltung rechtlicher Rahmenbedingungen aus vielerlei Gründen eine besonders wichtige Bedeutung zu. Dieser Bedeutung ist durch entsprechende vertragliche Regelungen Rechnung zu tragen. Darüber hinaus gibt es einige weitere Aspekte, die – insbesondere unter dem Aspekt eines effektiven Risiko-Managements sowie im Hinblick auf Steuerungs- und Kontrollfunktionen – zu beachten sind. Auf diese Punkte soll im Abschnitt 4.3 unter dem Aspekt der Vertragsgestaltung eingegangen werden.

Da ein Outsourcing-Projekt speziell auf die Situation beim Kunden zugeschnitten sein muss, wird es in absehbarer Zukunft wohl kein Template für einen Vertrag geben. Es ist jedoch zu erwarten, dass seriöse Anbieter von IT-Outsourcing mit vorgefertigten Vertragsteilen aufwarten, die die Compliance aus ihrer Sicht gewährleisten. Wegen ihrer Erfahrung aus einer größeren Anzahl von Projekten werden sie sich einen Vorsprung im Vertragswesen erarbeitet haben. Für Kunden ist es daher ratsam, sich im Vorfeld von Verhandlungen zumindest mit den grundlegenden Prinzipien (z.B. ITIL) auseinanderzusetzen und ggf. ITIL-Einführungskurse zu besuchen.

4.3.1 Schaffung einer Basis für eine langfristige Beziehung

Der Vertrag sollte so angelegt sein, dass er eine Basis für eine langfristige Zusammenarbeit zwischen dem Auftraggeber und dem Dienstleister darstellt. Es ist eine Zusammenarbeit zwischen Auftraggeber und Dienstleister auf Basis einer stabilen Geschäftsbeziehung anzustreben, in der ein kontinuierlicher und dokumentierter Informationsaustausch stattfindet.

4.3.2 Klare Definition und Abgrenzung der Verantwortlichkeiten

Wichtiger - häufig in seiner Bedeutung allerdings unterschätzter - Vertragsbestandteil ist eine klare Spezifikation der vom Dienstleister zu erbringenden Leistungen und der Verantwortlichkeiten des Dienstleisters sowie des Auftraggebers. Diese Spezifikation erfolgt in der Leistungsbeschreibung. Die Leistungsbeschreibung hat in erster Linie operative, daneben aber auch eine starke kaufmännische und rechtliche Bedeutung. Die Leistungsbeschreibung sollte daher zwischen den operativen, den kaufmännischen sowie den rechtlichen Einheiten der Vertragsparteien abgestimmt sein.

Häufig ist bei komplexen Outsourcing-Verträgen festzustellen, dass die Verantwortlichkeiten der Vertragsparteien gerade nicht klar genug definiert und voneinander abgegrenzt werden. Zu den

⁵¹Die nachfolgenden Klauselbeispiele dienen vornehmlich der Illustration und beinhalten jeweils nur Regelungen einzelner aus dem Kontext herausgelöster Punkte. Sie erheben keinen Anspruch auf Vollständigkeit und können eine konkrete Beratung im Einzelfall nicht ersetzen.

Aspekten, die insbesondere in der Leistungsbeschreibung bzw. den Service-Level-Agreements zu behandeln sind, gehören:

- Spezifikation von Annahmen und Prämissen
- Spezifikation der zu erbringenden Leistungen⁵²
- Spezifikation von Leistungsparametern (Key Performance Indicators (KPIs) sowie daran ausgerichteten Service Level Agreements (SLAs))
- Spezifikation der Verantwortlichkeiten (Mitwirkungs-/Beistelleistungen des Auftraggebers)
- Definition von Schnittstellen (prozessualer und technischer Art; Verantwortlichkeitsmatrix)
- Spezifikation einzuhaltender technischer und sonstiger Standards
- Bestimmung von Parametern, die eine Leistungsänderung auslösen.

Im Zusammenhang mit der Leistungsbeschreibung kommt der Festlegung und Messung von Leistungsparametern – sogenannten Key Performance Indicators (KPIs) - und daran ausgerichteten Service-Level-Agreements (SLAs), die quantitativer sowie qualitativer Art sein können, eine besondere Bedeutung zu. Der Sinn und Zweck dieser Festlegungen besteht zum einen darin, die spezifischen Anforderungen des Auftraggebers zu dokumentieren und zum Maßstab für die vom Dienstleister zu erbringenden Leistungen zu machen. In Kombination mit einem Berichtswesen, das den Auftraggeber regelmäßig über die (Nicht-)Einhaltung der vereinbarten Leistungsparameter informiert, wird zum anderen ein Kontroll- und Steuerungsmechanismus für den Auftraggeber gebildet. Die Nichteinhaltung von KPIs oder SLAs kann Auslöser für Vertragsstrafen oder (pauschalierten) Schadenersatz, Eskalationsprozesse oder Kündigungsrechte sein.

Wichtig bei der Vertragsgestaltung im Allgemeinen und bei der Festlegung der Leistungsbeschreibung sowie der SLAs im Besonderen ist, dass die Vertragsparteien das gleiche Verständnis von dem haben, was sie in den Vertragsdokumenten dokumentieren bzw. von dem, was sie nicht dokumentieren, was aber Grundlage ihrer Vertragsbeziehung ist. Ansonsten besteht regelmäßig die Gefahr eines versteckten Dissens, was dazu führen kann, dass der Vertrag gem. § 155 BGB im Zweifel als nicht geschlossen gilt. Die Orientierung an Standards wie ITIL (IT Infrastructure Library) hilft den Vertragsparteien, über einzelne Funktionen und Prozesse ein klares, gemeinsames Verständnis zu entwickeln.

4.3.3 Einhaltung rechtlicher Rahmenbedingungen

Ferner sollte geregelt werden, dass jede Vertragspartei in ihrer Sphäre für die Einhaltung der jeweils geltenden rechtlichen Rahmenbedingungen verantwortlich ist. Hierbei ist allerdings zu beachten, dass es im Einzelfall zweifelhaft sein kann, ob eine rechtliche Rahmenbedingung in die

⁵² ggf. explizite Definition von Leistungsausschlüssen, sofern zur Vermeidung von Missverständnissen erforderlich.

Sphäre des Auftragnehmers, des Auftraggebers oder gegebenenfalls beider Partner fällt. Dieser Graubereich ist zu verifizieren und im Vertrag zu adressieren. Bestehen unterschiedliche Auffassungen hinsichtlich der vertraglichen Pflichten der beiden Vertragsparteien, die sich im Zusammenhang mit der Einhaltung von rechtlichen Rahmenbedingungen ergeben, kann dies im Einzelfall einen versteckten Dissens i.S.v. § 155 BGB zur Folge haben – und der Vertrag gilt als nicht geschlossen.

Klauselbeispiel 1: Einhaltung der rechtlichen Rahmenbedingungen

1. Der Auftragnehmer wird die Leistungen in Übereinstimmung mit den [jeweils geltenden] rechtlichen Rahmenbedingungen⁵³ erbringen. Der Auftragnehmer gewährleistet, dass der Auftraggeber in der Lage ist, rechtlichen Rahmenbedingungen, die auf die Leistungen Anwendung finden, zu entsprechen.
2. Zur Vermeidung von Zweifeln stellen die Vertragsparteien klar, dass der Auftragnehmer [insbesondere] für die Einhaltung folgender rechtlicher Rahmenbedingungen verantwortlich ist: [...]. Der Auftraggeber ist [insbesondere] für die Einhaltung folgender Bestimmungen verantwortlich: [...].

4.3.4 Einhaltung spezieller rechtlicher Rahmenbedingungen und Standards

Standards, (technische) Richtlinien und Normen, auf deren Einhaltung es bei der Leistungserbringung besonders ankommt, sind ausdrücklich in den Vertragsdokumenten zu spezifizieren; in der Regel bietet sich hierfür die Leistungsbeschreibung an (vgl. Abschnitt 4.3.2). Im Zusammenhang mit der Einhaltung von Standards ist zu beachten, dass viele Standards „vom Markt vorgegeben“ werden und nicht gesetzlich geregelt⁵⁴ sind. Es ist zu regeln, welche Standards von wem einzuhalten sind⁵⁵. Allgemeine Klauseln wie „allgemein anerkannte Regeln der Technik“, „Stand der Technik“, „Stand von Wissenschaft und Technik“ oder „beste verfügbare Technik“ sind aufgrund ihrer Unbestimmtheit nicht eindeutig genug, vermitteln häufig nur eine Scheinsicherheit und sollten daher nur ergänzend verwendet werden.

Insbesondere muss der Auftragnehmer im Fall der Auftragsdatenverarbeitung gemäß § 11 Abs. 2 BDSG dazu verpflichtet werden, im Einzelnen (vorzugsweise in einer Anlage zum Vertrag) konkret und detailliert die technischen und organisatorischen Maßnahmen aufzuführen, die er zur Sicherstellung der Anforderungen gemäß § 9 BDSG und dessen zugehöriger Anlage ergreifen wird.

⁵³ Der Begriff „rechtliche Rahmenbedingungen“ sollte definiert werden: „Rechtliche Rahmenbedingungen“ sind alle Gesetze im formellen und materiellen Sinn (z. B. Verordnungen, behördliche Vorgaben und Bekanntmachungen, aufsichtsrechtlicher Anforderungen), Richtlinien und Standards, denen die Leistungen zu entsprechen haben.

⁵⁴ z. B. keine gesetzlichen Vorgaben für Firewalls, Virens Scanner.

⁵⁵ wie werden sie implementiert, wie angepasst, wie werden Kosten getragen.

Implementierung und Betrieb der technischen Lösung für das Outsourcing ergeben sich aus den Anforderungen des Kunden. Bei Software sollte eine am Markt etablierte und bei anderen Unternehmen zuverlässig eingesetzte Produktversion genutzt werden. Ein Festhalten an veralteten Standards oder der Einsatz vollkommen neuer Technologien erhöht das Risiko und sollte daher nur auf Basis einer soliden Risikobewertung stattfinden.

Klauselbeispiel 2: Technische und organisatorische Maßnahmen und Standards

1. Der Auftragnehmer wird zur Gewährleistung des Datenschutzes und der Datensicherheit die in Anlage [...] im Einzelnen spezifizierten technischen und organisatorischen Maßnahmen ergreifen und während der gesamten Zeit der Leistungserbringung aufrechterhalten. Insbesondere wird der Auftragnehmer die Daten gegen unbefugten Zugriff, unbefugte Veränderung, Vervielfältigung und sonstige unbefugte Nutzung sowie gegen Verlust schützen.
2. Ferner wird der Auftragnehmer die in der Leistungsbeschreibung definierten technischen Standards in der jeweils aktuellen Fassung über die gesamte Zeit der Leistungserbringung einhalten:
 - [...]
 - [...]
3. Die Kosten für die Ergreifung und Aufrechterhaltung der technischen und organisatorischen Maßnahmen sowie für die Einhaltung der Standards trägt der Auftragnehmer.

4.3.5 Umgang mit geänderten Anforderungen und rechtlichen Rahmenbedingungen

Aufgrund der schnellen technologischen Entwicklung⁵⁶, geschäftlichen Veränderungen beim Auftraggeber sowie Veränderungen von rechtlichen Rahmenbedingungen ist die nach einem Outsourcing-Vertrag zu erbringende Leistung in der Regel nicht statisch, sondern unterliegt während der Vertragslaufzeit zahlreichen Änderungen und Anpassungen.

Outsourcing-Verträge können nur bedingt alle möglichen Eventualitäten einer Vertragsbeziehung in der Zukunft abbilden. Dies bedeutet jedoch nicht, dass der Outsourcing-Vertrag diese Eventualitäten vernachlässigen kann und in überhaupt keiner Form zu adressieren hätte. Zu unterscheiden ist zwischen

- Änderungen, die bereits bei Vertragsabschluss antizipierbar sind und
- solchen, die noch nicht antizipierbar sind.

⁵⁶ z.B. weiterentwickelte technische Standards bei Hardware- oder Softwareherstellern.

Dort, wo Änderungen vorhersehbar sind, sollte versucht werden, die Folgen im Vorfeld möglichst genau zu definieren. Sich ändernde Anforderungen in Bezug auf den Leistungsumfang bzw. das Leistungsvolumen bei einem dynamischen Geschäftsumfeld lassen sich beispielsweise recht häufig durch ein entsprechend flexibles, vorab definiertes Preismodell erfassen.

Dort, wo sich solche Änderungen im Vorfeld nicht erfassen lassen, ist zumindest ein Verfahren festzulegen - in der Regel ein Change-Request-Verfahren -, das beschreibt,

- wer welche Änderungen initiieren kann,
- wie mit entsprechenden Änderungsanträgen umgegangen wird,
- wie geänderte Anforderungen des Auftraggebers einer Lösung zugeführt werden.

Für das Change-Request-Verfahren werden innerhalb der Governance-Struktur zwischen den Vertragsparteien die entsprechenden Gremien und deren Entscheidungsbefugnisse festgelegt.

Die Anpassung an geänderte rechtliche Anforderungen, die zwangsläufig umgesetzt werden müssen, wird - zumindest im Hinblick auf die operative Umsetzung⁵⁷ - in der Regel ebenfalls über das Change-Request-Verfahren gesteuert.

Hiervon zu trennen ist die Frage, wer von den Vertragsparteien in welchem Umfang die mit der Anpassung an die geänderten rechtlichen Anforderungen verbundenen Kosten⁵⁸ zu tragen hat. Insoweit ist insbesondere von Bedeutung, ob bzw. in welchem Umfang diese bereits vom vertraglich vereinbarten Leistungsumfang erfasst sind, d.h. ob und in welchem Umfang der Dienstleister das Risiko neuer oder geänderter Anforderungen trägt.

In der Regel handelt es sich hierbei im Ergebnis um eine kaufmännische Frage, bei deren Beantwortung es kein allgemeines „Richtig“ oder „Falsch“ bzw. eine Standardlösung gibt. So kann es bei Shared Services durchaus angemessen und sinnvoll sein, den Dienstleister – zumindest in einem bestimmten Umfang⁵⁹ – das Risiko neuer bzw. sich ändernder rechtlicher Rahmenbedingungen tragen zu lassen. Bei einer One-to-One Solution kann das schon wieder anders aussehen.

Wichtig ist zunächst einmal, dass dieser Aspekt geregelt wird. Die konkrete Ausgestaltung ist eine zweite Frage. Sofern wegen der Umsetzung geänderter bzw. neuer rechtlicher Rahmenbedingungen auf ein Änderungsverfahren Bezug genommen wird, sollte ausdrücklich geregelt sein, dass

⁵⁷ d.h. die Frage „wie“ wird die geänderte Anforderung umgesetzt.

⁵⁸ sowohl einmalige Kosten für die Implementierung der Änderung, als auch sich daran anschließende laufende Kosten für die geänderte Leistungserbringung.

⁵⁹ denkbar ist beispielsweise, mit einem Budget zu arbeiten, innerhalb dessen Grenzen die mit den Änderungen verbundenen Kosten vom Dienstleister zu tragen sind.

der Dienstleister grundsätzlich⁶⁰ zur Umsetzung der Änderung bzw. Neuerung verpflichtet ist und ggf. ein außerordentliches Kündigungsrecht des Auftraggebers besteht, wenn der Dienstleister der Umsetzungspflicht nicht nachkommt.

Für den Fall von Unstimmigkeiten sind Eskalationsprozesse als Teil der Governance im Vertrag zu definieren, die eine zügige Entscheidung ermöglichen.

Klauselbeispiel 3: Umgang mit geänderten oder neuen rechtlichen Bedingungen

1. Der Auftragnehmer überwacht die für die Leistungserbringung jeweils anwendbaren rechtlichen Rahmenbedingungen und teilt dem Auftraggeber jede anstehende Änderung einschließlich deren voraussichtlicher Auswirkungen auf die Leistungen frühzeitig [schriftlich] mit.
2. Aufgrund von geänderten oder neuen rechtlichen Rahmenbedingungen geänderte oder neue Anforderungen an die Leistungen wird der Auftragnehmer frühzeitig vor deren Inkrafttreten in Abstimmung mit dem Auftraggeber [nach Maßgabe des Änderungsverfahrens] umsetzen. Der Auftragnehmer ist nur bei Vorliegen eines wichtigen Grundes berechtigt, die Umsetzung der geänderten oder neuen rechtlichen Rahmenbedingung zu verweigern. Ein wichtiger Grund liegt [insbesondere] dann vor, wenn ... [Verweigert der Auftragnehmer die Umsetzung, ist der Auftraggeber zur Kündigung des Vertrages aus wichtigem Grund berechtigt.]
3. Hinsichtlich der mit der Anpassung verbundenen Kosten vereinbaren die Vertragsparteien [abweichend von den Regelungen des Änderungsverfahrens] folgendes: ... [kaufmännische Frage]

4.3.6 Notfallkonzepte

Für Outsourcing-Projekte, die dem § 25 a Absatz 2 KWG unterfallen, ist die Erstellung bzw. Pflege von Notfallplänen nach dem Rundschreiben 11/2001 ausdrücklich vorgeschrieben. Aber auch unabhängig von dem Anwendungsbereich von § 25 a Absatz 2 KWG sollte, insbesondere im Hinblick auf ein effizientes IT-Risiko- und Kontroll-Management, die Absicherung gegen und das Vorgehen im Notfall explizit geregelt sein. Dies umfasst

- einerseits die technische Absicherung gegen einen Notfall (Disaster Recovery Plan),
- ein Konzept zur Fortführung der kritischen Unternehmensprozesse (Business Continuity Plan) und andererseits
- die Implementierung eines Wiederanlaufplans (Business Recovery Plan).

⁶⁰ d.h. außer bei Vorliegen eines wichtigen Grundes, der anhand von Regelbeispielen soweit wie möglich konkretisiert, gegebenenfalls sogar abschließend definiert werden sollte.

Besondere Sorgfalt ist hierbei auf die Regelung der jeweiligen Verantwortlichkeiten und Entscheidungsbefugnisse sowie Abstimmungserfordernisse zu verwenden. Mittels entsprechender Vereinbarungen sollte auf eine regelmäßige Überprüfung und etwaig erforderliche Anpassung der Notfallplanung geachtet werden.

Anforderungen an Notfallkonzepte werden typischerweise in der Phase der Vertragsgestaltung zwischen den Vertragsparteien festgelegt und als Teil der Leistungen des Auftragnehmers aufgenommen. Art und Umfang der Anforderungen haben einen direkten Einfluss auf den Preis der Dienstleistung. Neben vorgeschriebenen Anforderungen - wie z.B. im Bereich der Kredit- und Finanzdienstleister (§ 25 a Absatz 2 KWG) - ist ansonsten jeweils ein Abwägen von Kosten und Nutzen sinnvoll. Hierzu werden typischerweise im Vorfeld Risikoabschätzungen durchgeführt und die Kosten zur Risikovermeidung gegenübergestellt.

Eine „absolute Sicherheit“ ist nicht realisierbar und zum anderen mit überproportionalem Aufwand verbunden⁶¹. Für eine wirtschaftlich sinnvolle Lösung sollte der Auftraggeber die Erfahrung des Dienstleisters nutzen. So kann er das Restrisiko und den Aufwand zur Risikominimierung in Balance halten.

Unabhängig von einem Notfallkonzept werden generelle Sicherheitsmaßnahmen festgelegt. Hierbei handelt es sich im IT-Bereich um Maßnahmen zur Erreichung der gewünschten Verfügbarkeit von IT-Systemen und der Sicherheit der Datenbestände. Hohe Anforderungen an die Verfügbarkeit haben auch hier direkten Einfluss auf die Kosten der IT-Systeme und damit auf den Preis der Leistung.

Im Markt existieren De-facto-Standards wie z.B. Virens Scanner und Firewalls, die typischerweise in den Vertragsvereinbarungen zu regeln sind.

Wenn ausgefeilte Notfallkonzepte nicht Teil der Anforderungen sind, muss der Dienstleister die Möglichkeit bieten, Kundendaten wiederherzustellen. Hier sind Vorsorgemaßnahmen, Mitarbeiterschulung, Kennzeichnungs-Systeme für Backups etc. wichtig.

⁶¹ Der Grenznutzen nimmt ab.

Klauselbeispiel 4: Notfälle

1. Der Auftragnehmer wird - in Abstimmung mit dem Auftraggeber – innerhalb von vier (4) Monaten nach Vertragsunterzeichnung geeignete Notfallpläne entwickeln und umsetzen, die der vorbeugenden Verhinderung eines Notfalls dienen, sowie die Fortführung kritischer Unternehmensprozesse und die Wiederaufnahme der uneingeschränkten Geschäftstätigkeit des Auftraggebers bei Notfällen⁶² sicherstellen.
2. Als Mindestorientierungsmaßstab werden dem Auftragnehmer die entsprechenden Regelungen und Prozesse des Auftraggebers zum Zeitpunkt des Vertragsschlusses zur Kenntnis geben (Anlage [...]: Notfallplanung und Sicherheitsrichtlinien des Auftraggebers). Der Auftragnehmer wird darüber hinaus folgende Vorgaben beachten: ..., Vorgaben des BSI-Grundschutzhandbuches, ...
3. Die Notfallpläne sind dem Auftraggeber [spätestens zum ...] zur Abnahme vorzulegen und werden nach Abnahme diesem Vertrag als Anlagen [...] bis [...] beigelegt.
4. Der Auftragnehmer wird die Notfallpläne soweit erforderlich, mindestens jedoch alle sechs (6) Monate, nach Absprache mit dem Auftraggeber überprüfen und bei Sicherheitsmängeln entsprechend anpassen. Über das Ergebnis jeder Überprüfung sowie aufgetretene Sicherheitsmängel wird der Auftragnehmer den Auftraggeber unverzüglich schriftlich informieren.
5. Die Kosten für die Erstellung, Umsetzung und die Überprüfung der Notfallpläne sowie die damit zusammenhängenden Berichte trägt der Auftraggeber/-nehmer [kommerzielle Frage].

Darüber hinaus ist in dem Vertrag sicherzustellen, dass

- es einen angemessenen Prozess zur systematischen Entdeckung, Analyse, Bewertung und Minderung von IT-Risiken gibt (IT-Risiko-Management),
- es ein angemessenes System zur Planung und Kontrolle des ordnungsgemäßen Betriebs, die Umsetzung der Maßnahmen des IT-Risiko-Managements eingeschlossen, gibt (IT-Kontroll-System),
- IT-Risiko-Management und IT-Kontroll-System im operativen Betrieb effektiv gesteuert werden und tatsächlich zu einer Minderung der IT-Risiken führen.

⁶² Der Begriff „Notfall“ sollte, wie alle vertraglichen Schlüsselbegriffe, definiert werden: „Notfall“ meint das Erreichen eines Zustandes oder den Eintritt eines Ereignisses, aufgrund dessen die Erbringung der vom Auftragnehmer geschuldeten Leistungen, gleich aus welchem Grund, aus vernünftig-objektiver Sicht eines Dritten gefährdet erscheint, beeinträchtigt oder unmöglich ist, oder beeinträchtigt bzw. unmöglich werden könnte.“

4.3.7 Berichtspflichten, Prüfungs- und Kontrollrechte

Damit ein Unternehmen und damit dessen Geschäftsleitung und ggf. Aufsichtsrat sich sicher sein kann, alle relevanten Anforderungen einzuhalten, genügt es nicht, den Auftragnehmer zur Einhaltung all dieser Anforderungen zu verpflichten. Vielmehr muss kontinuierlich eine entsprechende Überprüfung erfolgen. Die Überprüfung basiert im Wesentlichen auf zwei Komponenten:

- Berichts- und Informationspflichten des Auftragnehmers, wonach der Auftragnehmer den Auftraggeber regelmäßig über bestimmte Umstände (beispielsweise die Einhaltung von Service Levels, das Auftreten von Mängeln und Problemen etc.) zu informieren hat;
- die Möglichkeit einer Überprüfung durch den Auftraggeber. Der Auftraggeber sollte sich demgemäß Prüfungs-, Zugangs- und Kontrollrechte einräumen lassen. Gemäß § 11 Abs. 2 BDSG ist im Falle der Auftragsdatenverarbeitung der Auftraggeber sogar verpflichtet, sich vor Auftragsvergabe von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen gemäß der Anlage zu § 9 BDSG zu überzeugen. Auch § 25 a Abs. 2 KWG im Zusammenhang mit dem Rundschreiben 11/2001 fordert ausdrücklich die vertragliche Festlegung von Prüfungs-, Zugangs- und Kontrollrechten.

Die Überprüfung, inwieweit der Auftragnehmer der Einhaltung seiner Pflichten nachkommt, kann durch den Auftraggeber, durch von ihm beauftragte Dritte oder durch unabhängige Dritte erfolgen. Wichtig ist es in diesem Zusammenhang zu regeln,

- worauf sich die Kontrollrechte beziehen⁶³,
- wie und von wem die Kontrollrechte auszuüben sind,
- wer die mit der Durchführung der Kontrolle verbundenen Kosten trägt und
- was die Folgen einer Kontrolle sind bzw. sein können.

Das Grundprinzip der Leistungsvereinbarung sollte sich danach richten, dass der Dienstleister den Nachweis bzw. Funktionsweise der Service-Level-Vereinbarungen antritt, die die zugesagte Leistungsqualität widerspiegeln. Ergänzend kann es sinnvoll sein, dass der Dienstleister zeigt, wie unter „erschweren Bedingungen“ die Einhaltung der Service-Level-Vereinbarung ermöglicht wird. Eine solche Situation wäre z.B. der Ausfall eines wichtigen Know-how-Trägers – hier müsste die Verfügbarkeit von adäquatem Ersatz nachgewiesen werden. Hierbei werden im Vertrag die Anforderungen an den Dritten festgelegt, der Prozess zur Überprüfung definiert und die Handhabung der entstehenden Kosten festgelegt.

Die Überprüfung von Notfallkonzepten erfolgt normalerweise in regelmäßigen Abständen, meist halbjährlich oder jährlich. Dazu werden Notfallszenarien festgelegt und anhand des Notfallplanes

⁶³ Gibt es beispielsweise einen Bereich, der allein der Hoheit des Dienstleisters unterliegt und von der Kontrolle des Auftraggebers ausgenommen ist?

getestet. Dieser Prozess wird gemeinsam vom Auftraggeber und Dienstleister durchgeführt. In Einzelfällen kann zusätzlich ein neutraler Dritter den Test begleiten. Erfolgt die Überprüfung des Notfallkonzepts generell unter Mitwirkung von Dritten, wird dies im Vertrag geregelt. Wiederum wird die Anforderung an den Dritten festgelegt, der Prozess zur Überprüfung definiert und die Handhabung der entstehenden Kosten festgelegt.

Unabhängig von individuellen Vereinbarungen mit einzelnen Kunden haben viele Dienstleister ihre Rechenzentren oder andere Einrichtungen von unabhängigen Instanzen prüfen und zertifizieren lassen. Die Einhaltung von entsprechenden Normen ist zu prüfen und zu dokumentieren.

Eine Nichterfüllung der vereinbarten Pflichten wird typischerweise in Abhängigkeit von den Auswirkungen geregelt. Dies kann bei schwerwiegenden Verstößen bis hin zur außerordentlichen Kündigung des Vertrags durch den Auftraggeber und zu Schadensersatzansprüchen führen.

Klauselbeispiel 5: Berichtspflichten

Der Auftragnehmer wird die Einhaltung der für die Leistungen vereinbarten Leistungsparameter (Service Levels) fortlaufend messen und kontrollieren. Der Auftragnehmer wird auf eigene Kosten Messinstrumente installieren, die zur Messung und Kontrolle erforderlich sind.

Der Auftragnehmer wird die Ergebnisse der Messungen und Überprüfungen auswerten und dem Auftraggeber spätestens am dritten Werktag jedes Kalendermonats einen detaillierten Bericht über die in dem vorausgegangenen Monat erzielten Werte nach Maßgabe des als Anlage [...] beigefügten Musters übermitteln.

Klauselbeispiel 6: Weisungs-, Prüfungs- und Kontrollrechte

Der Auftragnehmer ist befugt, Weisungen zu treffen, die zur vertragsgemäßen Ausführung der Leistungen notwendig sind. Die Weisungen sind, außer in Notfällen, nur gegenüber dem Projektmanager des Auftraggebers zu erteilen. Hält der Auftraggeber Weisungen des Auftragnehmers für unzumutbar, so hat er seine Bedenken unverzüglich schriftlich geltend zu machen.

Der Auftragnehmer wird den Prüfern⁶⁴ des Auftraggebers jederzeit zu Prüfungs- und Kontrollzwecken umfassenden und unbeschränkten Zugang zu allen Personen, Räumlichkeiten sowie den unter seiner Kontrolle stehenden Dokumenten, Daten, Datenträgern und Systemen gewähren, die mit den Leistungserbringung in Zusammenhang stehen.

Der Auftraggeber wird, soweit er darauf Einfluss nehmen kann, die Durchführung von Prüfungen mit einem Vorlauf von [fünf (5)] Werktagen ankündigen, Prüfungen nur zu den allgemeinen

⁶⁴ Der Begriff „Prüfer“ ist zu definieren: „Prüfer“ sind eigene Mitarbeiter des Auftraggebers sowie mit der Prüfung beauftragte Dritte.

Geschäftszeiten [...] des Auftragnehmers vornehmen und bei den Prüfungen das Interesse des Auftragnehmers an einem möglichst ungestörten Betriebsablauf berücksichtigen.

Die Prüfer sind berechtigt, Dokumente und Datenträger unter Beachtung und zur Erfüllung des jeweiligen Prüfungszwecks zu vervielfältigen.

Der Auftragnehmer wird alle Personen, die sich gegenüber dem Auftragnehmer zur Geheimhaltung verpflichtet haben, von dieser Geheimhaltungsverpflichtung gegenüber den Prüfern freistellen.

Die Prüfungs- und Kontrollrechte der Prüfer erstrecken sich auf die Prüfung und Kontrolle der vertragsgemäßen Leistungserbringung und die Einhaltung der vertraglichen Bestimmungen und umfassen insbesondere:

- die Leistungsorte und sämtliche vom Auftragnehmer zur Erbringung der Leistungen eingesetzten Systeme, einschließlich deren Sicherheit,
- die Einhaltung der Service Level sowie die zur Überprüfung der Einhaltung der Service Level eingesetzten Tools und die aufgezeichneten Messergebnisse,
- die Sicherheit und den Schutz geheimhaltungsbedürftiger Daten, einschließlich der vom Auftragnehmer zur Gewährleistung der Datensicherheit und des Datenschutzes getroffenen technischen und organisatorischen Maßnahmen,
- die Einhaltung der für die Leistungserbringung relevanten rechtlichen Rahmenbedingungen durch den Auftragnehmer.

Vorbehaltlich weitergehender rechtlicher Rahmenbedingungen, sind die Prüfer bis [zwei (2)] Jahre nach dem Ende des Geschäftsjahres des Auftragnehmers, in dem die Kündigung des Vertrages wirksam wurde, zur Prüfung und Kontrolle berechtigt. Der Auftragnehmer stellt sicher, dass während dieses Zeitraums alle relevanten Dokumente und Datenträger vorhanden sind.

Der Auftragnehmer wird die Prüfer bei Ausübung ihrer Prüfungstätigkeit, soweit zumutbar, angemessen unterstützen.

4.3.8 Folgen der Vertragsbeendigung

In Anbetracht der regelmäßig hohen Relevanz der IT für das Unternehmen sollte bereits im Outsourcing-Vertrag möglichst detailliert geregelt werden, wie im Falle einer Vertragsbeendigung die Verfügbarkeit der benötigten IT-Leistungen unterbrechungsfrei und in der erforderlichen Zuverlässigkeit und Qualität sichergestellt wird. Bei der Vertragsbeendigung erfolgt typischerweise ein Re-Transition-Projekt. Hierbei werden - vergleichbar dem Vertragsbeginn - die Leistungen vom aktuellen Dienstleister auf den Auftraggeber zurück oder einen „Nachfolge-Dienstleister“ überführt. In Anbetracht von mehrjährigen Vertragslaufzeiten und zu erwartenden Änderungen am Leistungsumfang ist bei Vertragsgestaltung eine Re-Transition oft nicht genau

planbar. Weitere Unsicherheiten resultieren aus dem schnellen Fortschritt der Technologie. Gleichwohl bzw. gerade deshalb sind die generellen Verantwortlichkeiten⁶⁵ des Dienstleisters in der Re-Transition so umfassend wie möglich bereits im Outsourcing-Vertrag abstrakt festzulegen und bei Vertragsbeendigung im erforderlichen Umfang zu konkretisieren.

Das Re-Transition-Projekt wird prinzipiell parallel zum laufenden Betrieb durchgeführt, um an einem oder mehreren Terminen die Leistungserbringung an den Auftraggeber oder einen vom Auftraggeber benannten „Nachfolger-Dienstleister“ zu übergeben.

Neben dem eigentlichen Re-Transition-Projekt sollte im Vorfeld die Handhabung des Anlagevermögens (Hardware, Software), die Übertragung von Rechten (z. B. Lizenzen) und der Verträge mit Dritten (z. B. Softwarepflegeverträge, Hardwarewartungsverträge) geregelt werden. Zu denken ist darüber hinaus an Regelungen, wonach der Dienstleister zur Erbringung von bestimmten Unterstützungsleistungen verpflichtet ist (bspw. Datenmigration, Schulungen, Erteilung von Auskünften). Ferner kommt der Frage eines möglichen Betriebsübergangs nach § 613 a BGB, sei es auf den Auftraggeber, sei es auf den „Nachfolge-Dienstleister“ eine sehr große Bedeutung zu. Die deutsche und europäische Rechtsprechung zum Betriebsübergang beim sogenannten Second-Generation Outsourcing, d. h. der Auslagerung einer Leistung auf einen „Nachfolge-Dienstleister“ befindet sich zurzeit im Fluss und bedarf bei der Vertragsgestaltung größter Aufmerksamkeit.

Schließlich ist auch an eine Pflicht des Dienstleisters zu denken, wonach er die Leistungen auf Wunsch des Auftraggebers für einen Übergangszeitraum - unabhängig von einer vorangegangenen Beendigung/Kündigung des Vertrages - weiter erbringt, sofern der Auftraggeber einen entsprechenden Bedarf rechtzeitig geltend macht. Dies beispielsweise für den Fall, dass das Insourcing oder die Übertragung der Leistungen auf einen anderen Dienstleister – aus welchem Grund auch immer – nicht zu dem geplanten Termin abgeschlossen ist.

Klauselbeispiel 7: Exit Management

1. Auf Wunsch des Auftraggebers erbringt der Auftragnehmer alle Leistungen, die zur Überleitung der Leistungen auf den Auftraggeber oder einen vom Auftraggeber benannten Dritten erforderlich sind (z.B. die Migration auf ein anderes System, die Gestellung von entsprechend qualifizierten Mitarbeitern, die Durchführung von Schulungen). Der Auftragnehmer wird mit dem Auftraggeber bzw. den von dem Auftraggeber benannten Dritten eng zusammenarbeiten.

⁶⁵ Unterstützung bei der Planung und Durchführung des Projektes, Bereitstellung aktueller Betriebsdokumentationen und Handbücher.

2. Der Auftragnehmer wird alle Unterlagen, Datenträger und Daten in einem zugänglichen und lesbaren elektronischen Format an den Auftraggeber herausgeben oder nach entsprechender schriftlicher Aufforderung durch den Auftraggeber unwiederbringlich löschen.
3. Details des Exit Managements insbesondere Optionsrechte des Auftraggebers sowie der hierfür zu zahlenden angemessenen Vergütung regeln die Parteien in Anlage [...].
4. Sobald feststeht, dass der Vertrag beendet wird, werden die Vertragsparteien die näheren Einzelheiten bezüglich der vom Auftragnehmer zur Überleitung der Leistungen auf den Auftraggeber oder einen von dem Auftraggeber benannten Dritten zu erbringenden Unterstützungsleistungen in einem Exit-Plan vereinbaren.
5. Unabhängig vom Grund der Beendigung dieses Vertrages wird der Auftragnehmer auf Verlangen des Auftraggebers die nach diesem Vertrag geschuldeten Leistungen solange unterbrechungsfrei und in gleicher Qualität wie bisher weiter erbringen, bis der Auftraggeber die Leistungen auf einen anderen Auftragnehmer übergeleitet hat oder selbst erbringt[, längstens jedoch für einen Zeitraum von [...] Monaten].

5 Nachweise zur Erfüllung regulatorischer Vorgaben

Merksatz 4

Von Outsourcing-Kunden und –Anbietern werden vielfach Nachweise, Prüfzertifikate und Bescheinigungen für die Konformität zu Vorgaben und Anforderungen aus Gesetzen, Richtlinien und Standards erwartet. Wegen der Vielfalt der Zielgruppen solcher Nachweise sowie der Formate für Prüfungen und Ergebnisdarstellung gibt es weder eine standardisierte Prüfroutine, noch eine allgemeingültige Prüfbescheinigung. Vielmehr orientieren sich Art und Inhalt der Prüfberichterstattung und deren Kosten an den individuellen Anforderungen, mit denen Kunden und Anbieter konfrontiert sind. Trends zur Vereinfachung und Kostenverringerung sind erkennbar.

5.1 Übersicht

Für Kunden und Anbieter von Outsourcing reicht es nicht aus, den Vorgaben und Anforderungen aus Gesetzen, Richtlinien und Standards zu entsprechen. Oft müssen sie in Form einer externen Bestätigung den Nachweis vorweisen können, die eigenen Verpflichtungen zu erfüllen. Solche Nachweise, Prüfzertifikate und Bescheinigungen stehen im Mittelpunkt des Kapitels 5.

Welche Nachweise die beste Wirkung bei den Zielgruppen entfalten und wie ein Outsourcing-Dienstleister mit geringem Aufwand dazu kommt – auf diese Fragen gibt es keine einfachen Antworten. Zu vielfältig sind die Zielgruppen sowie die Formate der Durchführung von Prüfungen und der Darstellung ihrer Ergebnisse. Es gibt daher weder eine standardisierte Prüfroutine, noch eine allgemeingültige Prüfbescheinigung.

Art und Inhalt der Prüfberichterstattung orientieren sich folglich an den hochgradig individuellen Anforderungen, mit denen Kunden konfrontiert sind. Je schlechter es gelingt, diese Anforderungen einzugrenzen, desto mehr Handlungsbedarf und Aufwand entstehen bei Prüfung und Zertifizierung.

5.2 Umgang mit Prüfzertifikaten

5.2.1 Bescheinigungen aufgrund gesetzlicher Grundlagen und Vorgaben

Mit einzelnen Fachabteilungen oder die Geschäftsleitung gibt es innerhalb der geprüften Dienstleister zwei Zielgruppen für solche Bescheinigungen. Für die den Kundenservice leistende Fachabteilung des Providers steht der Nachweis von Qualität im Vordergrund - unternehmensintern und insbesondere zum Markt. Den Vertrieb interessiert im Wesentlichen die Außendarstellung, die Geschäftsleitung beides. Außerhalb des Dienstleisters ist es komplizierter – hier ist es sinnvoll, nach der Quelle und damit nach dem Zweck der Bescheinigungen zu unterscheiden in

- Bescheinigungen aufgrund von gesetzlichen Grundlagen oder Vorgaben von Aufsichtsbehörden (vgl. Abschnitt 3.3),
- Bescheinigungen nach Best Practice und Industrie-Standards,

- Bescheinigungen aus dem Umfeld der Jahresabschlussprüfung⁶⁶.

Bescheinigungen der ersten Gruppe haben für die Kunden eine hohe Bedeutung, da sie für die Einhaltung von Gesetzen letztendlich die alleinige Verantwortung tragen. Als Zielgruppen der Bescheinigungen treten hierbei abstrakt die "Öffentlichkeit" bzw. in letzter Instanz meist die Aufsichtsbehörden auf. Sie wollen erfahren, ob der Kunde den oftmals konkret vorgegebenen gesetzlichen und ordnungsrechtlichen Anforderungen entspricht und ob diese auch vom beauftragten Dienstleistungs-Unternehmen angemessen erfüllt werden.

5.2.2 Bescheinigungen nach Best Practice und Industrie-Standards

Externe Zielgruppen solcher Bescheinigungen sind Bestandskunden oder potentielle Geschäftspartner sowie die interessierte Öffentlichkeit. Sie wollen erfahren, ob sich die Arbeit des Kunden und seines Outsourcing-Dienstleisters als Ausdruck der von ihnen gebotenen Qualität an Standards (vgl. Abschnitt 3.5) oder Referenzmodellen (vgl. Abschnitt 3.6) orientiert. So wird sich ein Service-Provider die Umsetzung bzw. die Qualität der Umsetzung von ITIL durch einen unabhängigen Dritten bestätigen lassen, wenn viele Kunden bei ihm nach ITIL gestaltete Prozesse erwarten.

Anders als bei den gesetzlich oder aufsichtsrechtlich verankerten Vorschriften können hier die Dienstleister über die Schwerpunkte der Untersuchung und der Bescheinigung entscheiden. In ihrem Ermessen liegt es, ob Prüfbestätigung und Bescheinigung den eigenen Zielen entsprechen.

5.2.3 Bescheinigungen aus dem Umfeld der Jahresabschlussprüfung

Die Zielgruppen von Bescheinigungen dieser Art sind die Kunden und in der Regel deren Wirtschafts- oder Jahresabschlussprüfer. Ihr Interesse ist es zu erfahren, ob und inwieweit der Dienstleister den Kunden bei der Umsetzung einer ordnungsmäßigen und sicheren Buchhaltung (vgl. Abschnitt 3.5.1 bis 3.5.3) unterstützt. Soweit der Service-Provider hierzu nicht umfassend genug in der Lage ist, müsste der Kunde kompensatorische Maßnahmen ergreifen. Ihre Grundlage finden diese Anforderungen in den handels- und steuerrechtlichen Regelungen zur Ordnungsmäßigkeit. Die Bedeutung für den Adressaten ist daher hoch. Art und Inhalt von Prüfung und Nachweis orientieren sich auch hier an kundenindividuellen Anforderungen.

5.3 Standardisierung versus Individualisierung der Prüfung: Was treibt die Kosten?

Die Dienstleister - oft Auftraggeber für externe Prüfungen - und deren Kunden müssen entscheiden, ob

⁶⁶ Regelungen meist von berufsständischen Organisationen aus der Wirtschaftsprüfung.

- eine Standardisierung der Prüfung angestrebt werden sollte oder
- eine individuelle Prüfung zielführend ist

und sich dabei an den in Tabelle 7 angeführten Faktoren orientieren und eng miteinander abstimmen.

Tabelle 7: Standardisierte oder individualisierte Prüfung - Entscheidungsfaktoren

Faktor	Einzelfragen
Vielzahl gesetzlicher und sonstiger Einzelvorschriften	<ul style="list-style-type: none"> ■ Welche Vorschriften sind aus Sicht des einzelnen Kunden bedeutend und welche daraus resultierenden Teilanforderungen sind vom Dienstleister umzusetzen? Hinsichtlich welcher Vorschriften ist eine externe Prüfung und Bestätigung sinnvoll? ■ Aus Sicht der Dienstleister ist zudem zu klären, wie wichtig die Kundengruppen sind, die bestimmte Anforderungen als wesentlich ansehen.
Zielrichtungen und „Sichten“ verschiedener Prüfungs- und Zertifizierungs-Standards	<ul style="list-style-type: none"> ■ Welche Berichts- und Prüfungs-Standards (ISO, SAS 70) werden von den Kunden erwartet? ■ Welchen Aufwand verursacht die Prüfung nach diesem Standard für die Dienstleister selbst? ■ Welche Standards treffen Aussagen vorrangig zur Form und damit weitgehend unabhängig von den Inhalten⁶⁷? ■ Welche „Kontrollsicht“⁶⁸ ist bei an Best-Practice-Vorgaben orientierten Standards wichtig? ■ Ist eine Norm und deren Prüfung nur auf die Betrachtung eines Stichtages ausgerichtet? Wie wichtig ist in einem solchen Fall die Zeitperiode davor? ■ Gibt es ein einheitliches Verständnis der wichtigsten Begriffe?

⁶⁷ Im Extremfall besagt ein positives Prüfungsurteil dann nur, dass der Dienstleister seine Prozesse aufwändig und sorgfältig dokumentiert hat - eine Aussage zu deren Effizienz und Eignung für den angestrebten Zweck muss damit in keiner Weise verbunden sein.

⁶⁸ So fokussiert beispielsweise ITIL als Prozessmuster im IT-Bereich primär auf die Prozessgestaltung und kommt ohne detaillierte Vorschläge für Kontrollen aus, während CoBIT primär die Kontrollen betont - ohne sich detailliert auf die Prozesssicht einzulassen.

Faktor	Einzelfragen
Abhängigkeit des Umfangs und Aufwands einer Prüfung und Bescheinigung vom Standardisierungsgrad der Prozesse beim Dienstleister ⁶⁹	<ul style="list-style-type: none"> ■ Für welche Prozess- oder Unternehmensbereiche soll die Prüfung gelten, und welcher Standardisierungsgrad wird hierbei erreicht? ■ Für welchen Kreis der Kunden ist die Prüfung dann anwendbar - werden also gleiche Aufgaben für unterschiedliche Kunden nach gleichen Standards bearbeitet? ■ Hat der Dienstleister seine Prozess-Standards auf von Kunden übernommene Service-Bereiche übertragen? ■ Gelten die Prozess-Standards des Dienstleisters für alle seine Standorte?

Es leuchtet ein, dass die Kosten für eine Prüfung bzw. Bescheinigung umso geringer sein werden, je besser deren Eingrenzung gelingt. Der "Preis" dafür wird ein engerer Kundenkreis sein, für den die Bescheinigung werthaltig ist.

5.4 Was leisten einheitliche Zertifikate bereits heute - wo liegen Ziele?

Vereinheitlichung und Standardisierung von Prüfungen und Prüfbescheinigungen sind zurzeit nur in begrenztem Umfang möglich. In jedem Fall hängen die Möglichkeiten von den individuellen Gegebenheiten bei den Dienstleistern und den Anforderungen der Kunden ab.

"Was heute bereits geht" und zugleich den Trend für künftige Ziele setzt, ist in den letzten Jahren auch in Deutschland durch die Diskussionen um die SOX-Anforderungen deutlich vorangekommen. Als Prüfungs-Standard haben hierbei in Deutschland insbesondere SAS 70 und IDW PS 331 (vgl. S. 34) stark an Bedeutung gewonnen.

Diese Prüfungs-Standards haben folgende Gemeinsamkeiten:

- Die Normen und Detailanforderungen, die der Prüfung als Prüfungsmaßstab zugrunde gelegt werden, gibt das untersuchte Unternehmen - in der Regel in Abstimmung mit seinen Kunden - frei vor. Diese Vorgabe wird über so genannte "Kontrollziele" definiert, die die Anforderungen der Kunden widerspiegeln und für deren Erreichung der Dienstleister dann einsteht.
- Alle für das Verständnis dieser Kontrollziele und der zugehörigen Maßnahmen zu deren Erreichung erforderlichen Informationen werden im Prüfungsbericht dargelegt. Er umfasst die Kontrollziele selbst, eine Beschreibung der Prozesse und wesentlicher Kontrollen sowie die detaillierte Beschreibung der durch den Prüfer vorgenommenen Prüfungshandlungen.

⁶⁹ vgl. die Ausführungen zur Wertschöpfungsrelevanz im Abschnitt 2.2.

- Die Prüfung unterscheidet zwischen Sicherstellung der Maßnahmen zu einem Stichtag (as of date ...) und wahlweise zusätzlich der Bestätigung dieser Maßnahmen auch für einen rückblickenden Zeitraum. Insbesondere aus Revisionssicht ist es in der Regel nicht ausreichend zu wissen, wie "gut" der Dienstleister zu einem aktuellen Stichtag ist. Vielmehr ist hier auch von Bedeutung, ob die versprochene Qualität auch über die vergangene Periode hinweg konstant erbracht werden konnte.

Es ist auch jetzt schon möglich, dass der Dienstleister die für seine Kunden wichtigen Prüf- anforderungen in eine oder gezielt mehrere Prüfungen und Bescheinigungen integriert.

6 Datenschutzrechtliche Aspekte

Merksatz 5

Aufgrund der nach derzeitigem Rechtsstand herrschenden Komplexität von Datenschutzbelangen im Rahmen von Outsourcing-Verträgen ist die Einholung einer fundierten individuellen rechtlichen Beratung immer angezeigt.

6.1 Datenschutz bei Funktionsübertragung und Auftragsdatenverarbeitung

Besondere Bedeutung kommt regelmäßig dem Thema „Datenschutz“ zu, da mit dem Outsourcing typischerweise auch die Übermittlung bzw. Verarbeitung personenbezogener Daten verbunden ist⁷⁰. Problematisch ist, dass beim Outsourcing in der Regel zwei Unternehmen an der Verarbeitung personenbezogener Daten beteiligt sind, der Auftraggeber und Auftragnehmer. Wer dann schlussendlich für die Einhaltung welcher datenschutzrechtlichen Vorgaben verantwortlich ist, richtet sich danach, ob eine Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt.

Es muss daher zunächst immer die Frage gestellt werden, ob der Outsourcing-Anbieter zusätzlich zu den Datenverarbeitungsvorgängen auch die diesen zugrunde liegenden Aufgaben (oder einen Teil davon) übernimmt. Dabei handelt es sich um die so genannte Funktionsübertragung. Im Falle einer Auftragsdatenverarbeitung nimmt der Outsourcing-Anbieter eine Hilfsfunktion wahr und ist in seiner Tätigkeit ausschließlich auf die Abwicklung der Datenverarbeitungs-Prozesse beschränkt. Der Outsourcing-Anbieter handelt dabei weisungsgebunden.

Typische Beispiele für die Auftragsdatenverarbeitung⁷¹ sind:

- Outsourcing von Rechenzentren
- Kundenservice
- Datenträgervernichtung
- externe Gehaltsabrechnung
- manueller oder elektronischer Archivierungsservice.

Bei der Auftragsdatenverarbeitung ist der Auftraggeber der Verantwortliche für die Einhaltung des Datenschutzes, auch dann, wenn er die Daten nicht selbst erhebt oder verwaltet, sondern dies durch den Outsourcing-Anbieter erfolgt. Die Datenschutzverpflichtungen gehen nur im Falle der

⁷⁰ Vgl. Fußnote 17.

⁷¹ Unter http://www.bitkom.org/de/themen_gremien/36266_25976.aspx ist eine Mustervertragsanlage des BITKOM zur Auftragsdatenverarbeitung verfügbar.

Funktionsübertragung auf den Outsourcing-Anbieter über. Selbst hier bleibt aber der Auftraggeber zur sorgfältigen Auswahl des Anbieters verpflichtet.

Ein entscheidender Unterschied zwischen der Auftragsdatenverarbeitung und der Funktionsübertragung ist die Tatsache, dass bei der Auftragsdatenverarbeitung das Privileg der §§ 11, 3 Abs. 8 BDSG greift und hier keine weitere Einwilligung der Betroffenen erforderlich ist.

6.2 Datenübermittlungen oder -verarbeitungen im Ausland

Unabhängig von der Frage, wer für die Einhaltung des Datenschutzes verantwortlich ist, muss auch die Frage gestellt werden, wann der Datenschutz ausreichend berücksichtigt ist, insbesondere im Rahmen von Datenübermittlungen oder -verarbeitungen im Ausland. Wichtig ist daher, wohin die Daten übertragen werden bzw. wo die Daten verarbeitet werden. Die in Tabelle 8 dargestellten Varianten sind zu unterscheiden. Weitere Informationen enthält auch der BITKOM-Leitfaden „Übermittlung personenbezogener Daten– Inland, EU-Länder, Drittländer“ (vgl. http://www.bitkom.org/de/publikationen/38337_39321.aspx).

Tabelle 8: Varianten zur Gewährleistung des Datenschutzes

Datenübertragung innerhalb der EU	Die erste Möglichkeit, der Datentransfer bzw. die Datenverarbeitung innerhalb der EU, ist die Variante ohne Probleme. Europaweit gelten vergleichbare Datenschutzgesetze, die auf der EU-Richtlinie 95/46 EG basieren ⁷² . Davon umfasst sind auch die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum.
Angemessenheitsentscheidungen der EU-Kommission	Darüber hinaus hat die Europäische Kommission in Einzelfällen entschieden, in welchen Ländern ein angemessenes Datenschutzniveau herrscht. Dazu zählen zum Beispiel die Schweiz, Argentinien sowie die Kanalinseln Guernsey, Jersey und Isle of Man. Lediglich zum Teil fällt darunter auch Kanada, nicht jedoch die USA. In Staaten mit einem angemessenen Datenschutzniveau ist ein Datentransfer bzw. die Verarbeitung personenbezogener Daten unproblematisch.
U.S. „Safe Harbor“-Programm	Im rechtskonformen Raum bewegt man sich auch bei Unternehmen, die sich an dem so genannten „Safe Harbor“-Übereinkommen beteiligen. EU-Kommission und das U.S. Handelsministerium haben sich darauf verständigt, dass dem europäischen Datenschutz dann Genüge getan ist, wenn sich private Unternehmen dem „Safe Harbor“-Übereinkommen unterwerfen und sich damit selbst verpflichten, den Richtlinien des

⁷² Unter http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm sind weitere Informationen von der Europäischen Kommission zum Datenschutz verfügbar.

	<p>europäischen Datenschutzes Rechnung zu tragen. Leider gilt diese Regelung bisher nur in den Vereinigten Staaten, so dass man sich bei einem Datentransfer in das nicht-europäische und nicht-amerikanische Ausland weiteren Reglements bewusst sein sollte.</p>
<p>EU-Standard- vertragsklauseln</p>	<p>Eine weitere Möglichkeit des gesetzeskonformen Verhaltens bieten die EU-Standardvertragsklauseln (§ 4 c Abs. 2 BDSG). Der ausländische Anbieter verpflichtet sich hier ähnlich dem Safe-Harbor Übereinkommen zur Einhaltung der europäischen Datenschutzrichtlinien. Ein ausländischer Auftragsdatenverarbeiter wird hierbei zur Vornahme von technischen und organisatorischen Sicherheitsmaßnahmen verpflichtet sowie dazu, nur nach Anweisung zu handeln. Schließt man eine solche Klausel mit seinem Vertragspartner ab, bedarf es in Deutschland keiner weiteren Überprüfung oder Anzeige an die Datenschutzbehörden. Der klare Vorteil dieser Klauseln ist, dass sie weltweit einsetzbar sind, ganz im Gegensatz zu den rein auf die Vereinigten Staaten beschränkten Safe Harbor Unternehmen. Wichtig hierbei ist, dass man sich an den genauen Wortlaut der Klauseln hält. Nur so bleibt man von einer Genehmigungspflicht verschont.</p>
<p>Verbindliche Unternehmens- regelungen</p>	<p>Die verbindlichen Unternehmensregelungen, zum Teil Data Protection Code of Conduct genannt (§ 4c Abs. 2 BDSG), bieten ebenfalls eine Variante zur Einhaltung des europäischen Datenschutzniveaus. Hier kann ein Konzern sich selbst ein Regelwerk aufstellen, das den Umgang mit personenbezogenen Daten, wie zum Beispiel Kundendaten, Arbeitnehmerdaten oder Bewerberdaten in dem gesamten Konzern regelt. Dies muss dann von den Datenschutzbehörden genehmigt werden. Allerdings ist momentan noch eine Genehmigung einer jeden Datenschutzbehörde der betroffenen EU-Mitgliedstaaten erforderlich, ein aufwendiges Unterfangen also. Für die Zukunft werden hier Erleichterungen in Aussicht gestellt: So soll hoffentlich bald die Genehmigung einer einzigen europäischen Datenschutzbehörde ausreichend sein, was das Verfahren deutlich erleichtern würde - ein längst überfälliges Vorgehen, da der Datenschutz schließlich auf einer europäischen Richtlinie beruht.</p>
<p>Einwilligung der Betroffenen</p>	<p>Grundsätzlich ist die Datenübermittlung/ oder -verarbeitung immer dann zulässig, wenn der Betroffene einwilligt (§ 4, 4a, 4 c BDSG). Einwilligen kann der Betroffene allerdings nur dann, wenn er ausreichend informiert wurde. Die Einwilligung selbst muss klar und ausreichend bestimmt sein. Sie wird in aller Regel schriftlich abgegeben. Das Datenschutzgesetz fordert auch, dass die Einwilligung auf freien Stücken eines Einzelnen beruht. Dies wird insbesondere im Bezug auf Arbeitsverhältnisse umstritten diskutiert. Häufig wird hier die Freiwil-</p>

lichkeit aufgrund des Abhängigkeitsverhältnisses in Frage gestellt. Ein ausreichender Kontrollmechanismus existiert hier nicht. Zur Lösung dieses Problems wird häufig vorgeschlagen, eine Betriebsvereinbarung mit dem Arbeitnehmervertreter abzuschließen. Dies geht allerdings nur in Unternehmen, in denen auch ein Betriebsrat vorhanden ist. Bei allen anderen wird eine möglichst umfassende, klare und schriftliche Einwilligung eines jeden einzelnen Betroffenen gefordert.

7 Fallbeispiele für die Anwendung von Richtlinien, Standards und Referenzmodellen

Merksatz 6

Fallbeispiele sind hilfreich, die vergleichsweise abstrakten gesetzlichen Anforderungen besser zu verstehen. In Form von Best Practice sind handlungsorientiert Erfahrungen aus der Praxis komprimiert. So kann gezeigt werden, dass sich eine Vielzahl von regulatorischen Vorgaben bereits durch sorgfältige Gestaltung der Service-Level Agreements und Verträge zwischen Outsourcing-Kunden und –Anbietern beherrschen lässt.

7.1 Einführung – zum Erkenntnisgewinn aus Fallbeispielen

Im Kapitel 3 wurde dargestellt, dass die i.d.R. generisch gehaltenen gesetzlichen Anforderungen in vielen Fällen durch Richtlinien und Standards näher spezifiziert und konkretisiert werden. Sie können die Umsetzung der gesetzlichen Anforderungen in der Praxis unterstützen. In wenigen Fällen jedoch können erwähnte Zertifikate oder Prüfungsbestätigungen Dritter den Nachweis zur Erfüllung gesetzlicher Anforderungen liefern. Sie werden meist nur für einen definierten Prozess und einen vorbestimmten Zeitraum abgegeben. Die ständige Überwachung der Compliance bleibt demnach weiter bei der Unternehmensleitung.

Aus diesem Grund werden im Kapitel 6 einige Beispiele für die Anwendung der in den vorangegangenen Kapiteln beschriebenen Richtlinien, Standards und Referenzmodelle zusammengestellt. Um den Praxisbezug besser darzustellen, hilft es, die zahlreichen Anforderungen den konkreten Problembereichen zuzuordnen:

- Wie wird z.B. ein entsprechendes IT-Sicherheitsniveau oder die Einführung eines Risiko-Managements im Unternehmen gewährleistet?
- Mit welchen Mitteln führe ich Datenschutzmaßnahmen ein?
- Wie führe ich ein internes Kontroll-System ein?

Diese Fragestellungen wurden dann in den Praxisbeispielen den korrespondierenden Gesetzen, Richtlinien, Standards oder Referenzmodellen zugeordnet.

Die thematische Klassifizierung gesetzlicher Anforderungen – also die Zusammenfassung der verschiedenen Gesetze, Standards und Richtlinien in Gruppen mit ähnlichem inhaltlichen Fokus – erleichtert das Verständnis, was im Einzelnen für das betroffene Unternehmen und den entsprechenden Geschäftsprozess relevant ist.

In den meisten Fällen geht es um thematische Fragestellungen der internen Kontrolle über kritische Prozesse. Aspekte des Risiko-Managements, der internen Revision, der IT-Sicherheit oder

auch Datenschutz-Fragestellungen müssen beantwortet werden. Dabei handelt es sich hier lediglich um Schwerpunkte, und die Übergänge sind fließend.

Die nachfolgenden Fallbeispiele sollen verdeutlichen, welche Prozesse, Aufgaben und Inhalte in den konkreten Fällen in die Betrachtung einbezogen wurden. Die gesetzlichen Anforderungen selbst geben über die einzuleitenden Maßnahmen keine Hinweise, denn es bleibt am Ende immer in der Verantwortung der Geschäftsleitung, die eigenen Risiken zu benennen und entsprechende Maßnahmen einzuleiten. So müssen Entscheidungen, welche Bereiche der physischen RZ-Infrastruktur, welche Systeme und Betriebs- sowie Service-Prozesse für Fragen der internen Kontrolle, des Datenschutzes oder der IT-Sicherheit relevant sind, für jede Maßnahme und für jede Zertifizierung oder Prüfung individuell getroffen werden.

7.2 Fallbeispiel 1 - IT-Sicherheit

7.2.1 Gesetzliche Anforderungen und Unternehmensdarstellung

Das Fallbeispiel betrifft die Umsetzung von KonTraG, KWG, Basel II u.a.

Das Unternehmen ist mit knapp 230 Mitarbeitern eine kleine, in Deutschland notierte Aktiengesellschaft mit einem Umsatz von 30 Mio Euro. Kernkompetenzen liegen

- im Agenturgeschäft,
- in der Prozessberatung und in IT-Infrastruktur-Services,
- in der der Planung, Implementierung und im Betrieb von digitale Informations-, Kommunikations- und Vermarktungslösungen.
- Dazu kommen Beratung und die Bereitstellung von RZ -Leistungen.

Die Geschäftstätigkeit ist auf den deutschen Markt ausgerichtet.

7.2.2 Ausgangssituation und Überlegung zur Auswahl eines Standards

Für die Sicherheit und Qualität seiner IT-basierten Geschäftsprozesse soll der Geschäftsbereich Informationstechnologie durch die TÜV Industrie Service GmbH, TÜV Rheinland Group, nach British Standard BS 7799-2:2002 zertifiziert werden. Die Norm ist der international anerkannte Standard für die Bewertung der Sicherheit von IT-Umgebungen (vgl. S. 36). Geprüft wird insbesondere die Security Policy, die Systementwicklung und Wartung sowie die personelle, physische und umgebungsbezogene Sicherheit. Das hier avisierte Zertifikat der IT-Sicherheit korrespondiert mit den Anforderungen, die sich aus dem KonTraG, KWG und Basel II ergeben.

BS 7799 setzt sich in Europa momentan immer mehr durch und wird auch von ISO 17799 abgebildet. Er berücksichtigt alle wesentlichen Aspekte der Unternehmens-, IT- und Daten-Sicherheit, aber auch gesetzliche Rahmenbedingungen und definiert eine Sicherheitspolitik als Leitlinie mit entsprechenden messbaren Sicherheitszielen, die monatlich sowie im jährlichen Wiederholungs-Audit überprüft werden. BS 7799 legt also einerseits sicherheitsrelevante Prozesse fest und macht

deren Überprüfung möglich, bietet aber andererseits die Möglichkeit für einen kontinuierlichen Verbesserungsprozess (KVP).

Der Sicherheitsstandard BS 7799 befasst sich konkret mit folgenden Schwerpunkten:

- Sicherheitspolitik
- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebes
- Zugangskontrolle
- Systementwicklung und -wartung
- Management des kontinuierlichen Geschäftsbetriebs
- Einhaltung der Verpflichtungen

Der internationale Standard ISO 27001⁷³ beschreibt die Grundsatzanforderungen an das Management - d.h. Planung, Realisierung, Überwachung und kontinuierliche Verbesserung - der Informations-Sicherheit in einem Unternehmen. Durch die zusätzliche Einbeziehung

- der ISO 17799 (auf Maßnahmenebene) sowie
- der Standards der Familie ISO 13335 (auf der Ebene der Methodik)

entsteht eine praxisorientierte Vorgehensweise zur Gewährleistung von Informations-Sicherheit in einem Unternehmen.

Ein wesentliches Element eines Informations-Sicherheits-Managements nach ISO 27001 ist das Risiko-Management, das auf der systematischen Erkennung von Risiken an Hand von Risikoanalysen und Risikobewertungen basiert. Auf der einen Seite ermöglicht nur ein funktionierendes Risiko-Management den Einsatz stets angemessener, auch wirtschaftlich vertretbarer Informations-Sicherheits-Maßnahmen. Auf der anderen Seite besteht für jede Organisation die Herausforderung, das Informations-Risiko-Management in bereits bestehende Strukturen und Abläufe des Unternehmens zu integrieren.

Die Erfüllung der Anforderungen an den Managementrahmen für Informations-Sicherheit einer Organisation sowie an die Implementierung von adäquaten Sicherheitszielen und -maßnahmen⁷⁴

⁷³ Nachfolger des britischen Standards BS 7799-2.

⁷⁴ „security objectives and controls“.

eröffnet jedem Unternehmen den Weg zu einer zukunftsweisenden Zertifizierung des eigenen Informations-Sicherheits-Management-Systems (ISMS) nach dem internationalen Standard ISO 27001.

Gesetzlich relevante Bereiche umfassen neben Anforderungen des Datenschutzes (TDG, TKG etc), die rechtlichen Anforderungen kundenseitig auf Verfügbarkeit der IT-Dienstleistungen. Sicherheitskonzepte müssen ganzheitlich angelegt sein, wenn sie den Anforderungen der Zukunft standhalten sollen. Zertifizierte Sicherheit hat sich in datenintensiven Branchen zum Schlüsselfaktor für erfolgreiche Geschäftsbeziehungen entwickelt.

Ziel der Zertifizierung ist es, durch festgelegte Verfahren und Prozesse eine sichere Informationsverarbeitung zu dokumentieren. Die Zertifizierungen haben immer nur einen zeitlich begrenzten Gültigkeitsraum und müssen danach durch erneute Überprüfungen der Zertifizierer erneuert werden.

Neben einer BS-7799-Zertifizierung würde eine Zertifizierung nach dem IT-Grundschutzhandbuch des deutschen BSI ähnliche Ziele verfolgen, d.h. es ergeben sich verschiedene Handlungsalternativen das avisierte Ziel zu erreichen. Im Vergleich zu ähnlichen Standards wie dem BSI oder ISO 13335, beschränkt sich BS 7799 nicht auf IT-Sicherheit, sondern beschäftigt sich allgemein mit Informations-Sicherheit. Kein anderer Standard fordert so konsequent die kontinuierliche Verbesserung eines Management-Systems.

In diesem Fall wird eine Zertifizierung nach BS 7799 als sinnvoller erachtet, als eine Zertifizierung nach BSI, da insbesondere Kunden mit nicht deutschen Stammhäusern die BSI-Zertifizierung im Ausland nicht kennen oder nicht als ausreichend empfinden.

Die BS 7799 befindet sich gerade in einem Prozess der Umstellung auf eine ISO Norm - zertifiziert wird dann nach ISO 17799-2. BS 7799 wird über seine Ausprägung in ISO 17799 vor den anderen Normen am Markt durchsetzen und eine ähnliche Bedeutung wie ISO 9000 im Qualitäts-Management und ISO 14000 im Umweltschutz erreichen wird.

Es werden heute bereits die Datenschutzvorgaben durch einen Datenschutzbeauftragten umgesetzt. Das Unternehmen ist bereit nach ISO 9001 zertifiziert und der IT-Leiter nach ITIL ausgebildet. Das Unternehmen strebt eine Zertifizierung innerhalb von sechs Monaten an. Der nächste Jahresabschluss soll bereits den Hinweis auf die erfolgte Zertifizierung beinhalten.

Das BS 7799-Zertifikat soll darüber hinaus bei den Shareholdern und Kunden Vertrauen in das Sicherheits-Management erzeugen, wie es in der Natur eines solchen Zertifikats liegt. Besonders wichtig ist dabei der Auditor. Man muss sich also während des gesamten Projekts vergegenwärtigen, wie ein bislang unbeteiligter Dritter das implementierte System aus seiner Warte beurteilen würde. Auf diese Weise können Methoden entwickelt werden, die der Vermittlung von Sicherheitskonzeptionen dienen und somit Vertrauen nach außen schaffen.

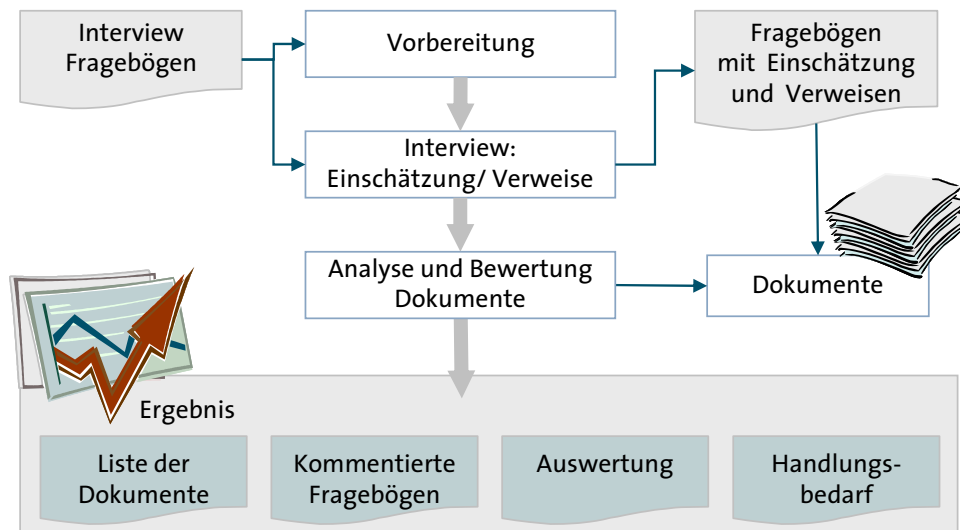


Abbildung 2: Interne Projektvorbereitung

7.2.3 Projektablauf

In einem ersten Schritt wird ein internes Audit durchgeführt. Ein Audit ist eine regelmäßige Überprüfung der Sicherheitsmassnahmen auf Übereinstimmung mit Sicherheitspolitik und Sicherheitsrichtlinien. Die Überprüfung erfolgt gegen Unternehmensrichtlinien, gegen Standards (BSI-Grundschutz / ISO17799 / ISO13335) und „Stand der Technik“ in vergleichbaren Unternehmen. Das Ergebnis ist ein priorisierter Überblick über den Handlungsbedarf und ein Überblick über die notwendigen Maßnahmen. Diese Audits können durch vertiefende Audits mittels detaillierter Checklisten, Penetrationstests, Hands-On Prüfungen von IT-Security Systemen, Einsatz von Software-Werkzeugen zur Systemüberprüfung ergänzt werden.

Zu Beginn des Projektes wird eine Gap-Analyse durchgeführt, um offensichtliche Schwachstellen festzustellen.

Im Betriebs- und Sicherheitskonzept wird beschrieben, auf welche Weise die Ausfallsicherheit des Systems gewährleistet wird. Die Organisation der Sicherheit wird hinterfragt und die Frage der personellen Sicherheit ist zentraler Bestandteil des Systems. Geregelt sind unter anderem auch die Sicherheit der Umgebung, die Kommunikation, das Management des Betriebs, die Zugangskontrolle sowie das Management des kontinuierlichen Geschäftsbetriebs.

Hierfür dokumentiert das Betriebs- und Sicherheitskonzept beispielsweise die verpflichtende SSL-Verschlüsselung der kompletten Datenübertragung, die Firewall- und Virenschutzlösungen sowie die Password-Policy und die Regeln zur Vergabe von Administratorenrechten.

Berücksichtigt werden auch die Monitoring-Prozesse, das heißt die automatisierte Systemüberwachung⁷⁵, sowie die Bedingungen, unter denen weitere externe Dienstleister für Supportaufgaben hinzugezogen werden können. Ziel ist, so viele Administratoren wie nötig, aber so wenig wie möglich zu involvieren. Dabei wird beispielsweise darauf geachtet, dass externe Partner nur über genau definierte Zeitfenster Zugang zum System haben. Darüber hinaus ist festgelegt, dass eine strikte Trennung zwischen den Produktivsystemen und den entsprechenden Entwicklungs- und Testumgebungen erfolgt.

Auf Basis der in der Gap-Analyse evaluierten Lücken wird ein Maßnahmenkatalog erstellt und die notwendigen Schritte zu deren Umsetzung eingeleitet. Abschließend erfolgt eine Abnahme der Geschäftsleitung.

7.2.4 Zertifizierungsprozess

Das Zertifizierungsschema zur Erlangung einer BS 7799-2:2002 Zertifizierung ist streng reglementiert. Die Zertifizierung darf nur durch speziell akkreditierte, sogenannte „Certification bodies“ erfolgen. Die Akkreditierung dieser „Certification bodies“ obliegt den nationalen Akkreditierungsstellen, in Deutschland ist dies die Trägergemeinschaft für Akkreditierung GmbH (TGA) in Frankfurt. Die nationalen Akkreditierungsstellen treffen gegenseitige Anerkennungsvereinbarungen, so dass die in einem Land ausgestellten Zertifikate auch in anderen Ländern Anerkennung finden. Die Akkreditierung der „Certification bodies“ erfolgt dabei gemäß der Richtlinie EA 7/03 der „European co-operation for Accreditation“. Zurzeit gibt es in Deutschland drei Unternehmen, die eine entsprechende Akkreditierung zur Durchführung von Zertifizierungen nach BS 7799-2 erhalten haben.

Die eigentliche Zertifizierung erfolgt dann prinzipiell nach folgendem Ablaufschema:

- Das zu zertifizierende Unternehmen beauftragt ein akkreditiertes Unternehmen - in diesem Fall die TÜV Industry Service GmbH - mit der Überprüfung des Information-Security-Management-Systems.
- Das Audit-Team wird zusammengestellt.
- In einer ersten Phase erfolgt die Überprüfung und Beurteilung der Dokumentation.
- In einer zweiten Phase werden Vor-Ort-Audits durchgeführt.
- Es wird ein Audit-Bericht erstellt.
- Sofern der Audit-Bericht positiv ausfällt, wird das Zertifikat ausgestellt.

⁷⁵ Betriebssysteme, Datenbanken, Anwendungsprozesse, Log-Files etc.

Das Zertifikat besitzt eine Gültigkeit von 3 Jahren. Anschließend ist eine Wiederholungs-Zertifizierung erforderlich, wodurch die Gültigkeit um weitere 3 Jahre verlängert wird.

7.3 Fallbeispiel 2 - Interne Kontrollprozesse

7.3.1 Gesetzliche Anforderungen und Unternehmensdarstellung

Die gesetzlichen Anforderungen werden durch den Sarbanes-Oxley-Act u.a. Gesetze bestimmt. Der Kunde ist Teil einer Unternehmensgruppe und deutschlandweit einer der führenden Anbieter auf dem Gebiet der Gebäude-, Anlagen- und Prozesstechnik sowie im Anlagen- und Gebäude-management. Das Unternehmen hat seine Zentrale in einer deutschen Großstadt. Die weiteren 14 Niederlassungen sind über ganz Deutschland verteilt. Mit etwa 800 Mitarbeitern erwirtschaftete das Unternehmen im Jahr 2005 einen Umsatz von circa 180 Mio. Euro.

Die Unternehmensgruppe ist als börsennotiertes Unternehmen in den Bereichen Energie und Umwelt weltweit führend und erzielte im Jahr 2005 mit mehr als 160.000 Mitarbeitern in über 100 Ländern rund 41,5 Mrd. Euro Umsatz. In Deutschland ist die Gruppe mit Tochterunternehmen in den Gebieten Strom und Gas, Fernwärme und Energiedienstleistungen, Wasser sowie Entsorgung tätig.

7.3.2 Ausgangslage

Die Personalabrechnung für ca. 840 aktive Mitarbeiter, Angestellte und gewerbliche Mitarbeiter sowie ca. 700 Rentner wurde durch SAP Human Resources (HR) als Mandant auf dem SAP R/3 ASP-System des Service-Providers vereinbart. Im Fokus stand zunächst der Einsatz der Komponenten Stammdatenverwaltung und Entgeltabrechnung. Zum anderen wurde die Auslagerung der Lohn- und Gehaltssachbearbeitung an die Service Unit des Dienstleisters im Rahmen eines Business Process Outsourcing (BPO) beschlossen. Zusätzlich wurde der Basisbetrieb des SAP R3 ERP Systems sowie der Betrieb zweier Server für Non-SAP-Anwendungen übertragen.

Der Kunde unterliegt über die Muttergesellschaft den SOX-Vorschriften. Da das Unternehmen die Personalabrechnung seiner Mitarbeiter an den Provider ausgelagert hat, beziehen sich die erforderlichen Wirtschaftsprüfungen damit ebenfalls auf die von den Konzerngesellschaften beauftragten Dienstleister. Es besteht die Möglichkeit, für die auf den Dienstleister entfallenden Kontrollen die Vorlage einer SAS 70 Bescheinigung vom Dienstleister anzufordern. Eine SAS 70 Zertifizierung würde in diesem Fall dem Management des Unternehmens den unabhängigen Nachweis ermöglichen, dass der beauftragte Dienstleister die in Section 404 des im SOX festgelegten Anforderungen erfüllt.

7.3.3 Projektinhalt

Für das konkrete Projekt ist zu berücksichtigen, dass nur ein enger Ausschnitt ausgelagert werden soll, nämlich der Unterbereich HR Management / Payroll Administration. Entsprechend begrenzt

ist der Prüfungsumfang, da im Rahmen der Anforderungen des SOX eigentlich nur sichergestellt werden muss, dass korrekte Daten bezüglich der Lohnabrechnung erzeugt und verwendet werden und dies auch kontrollierbar ist.

Während der Service-Provider also selbst keiner SOX-Prüfung unterliegt, ist er dennoch in seiner Eigenschaft als Dienstleister Gegenstand der SOX-Prüfung des Unternehmens. Die gemäß SOX kontrollierte Konzerngruppe hat in diesem Fall mehrere Handlungsoptionen, die kurz skizziert werden sollen:

- Das gemäß SOX kontrollierte Unternehmen kann einen Dienstleister einsetzen, der selbst nach SAS 70 zertifiziert ist⁷⁶. Die zu erfolgende Prüfungsnotwendigkeit kann sich durch die SAS 70 Bescheinigung auf ein Minimum reduzieren, sofern der entsprechende Wirtschaftsprüfer die Inhalte der SAS 70 Bescheinigung für seine eigene Prüfung mit verwendet.
- Das gemäß SOX kontrollierte Unternehmen kann einen nicht-zertifizierten Dienstleister einsetzen. Dieser Dienstleister muss dann aber die entsprechenden Kontrollen durch den Auditor des auftraggebenden Unternehmens ermöglichen und dafür auch ausreichende Ressourcen zur Verfügung stellen. In diesem Zusammenhang sind insbesondere die Anforderungen an das interne Überwachungssystem und an die interne Revision von Interesse. Über diese Kontroll-Systeme soll sichergestellt werden, dass die Prozesse in den Unternehmen ordnungsgemäß ablaufen und insbesondere Unregelmäßigkeiten nicht vorkommen oder - soweit doch Unregelmäßigkeiten auftreten - diese entdeckt und beseitigt werden. Diese beiden Systeme haben folgende Aufgaben:
 - Internes Überwachungssystem
Das interne Überwachungssystem soll den ordnungsgemäßen Ablauf der Prozesse überwachen.
 - Interne Revision
Aufgabe der internen Revision ist insbesondere die Kontrolle, ob das interne Überwachungssystem ordnungsgemäß arbeitet.

Auch beim Service-Provider gibt es Überwachungssysteme, die den SOX-Vorgaben entsprechen und auch zertifiziert werden:

- Risiko-Management:
Der Vorstand der Gesellschaft ist gemäß § 91 Absatz 2 AktG verpflichtet, ein Überwachungssystem einzurichten. Dieses System besteht beim beauftragten Dienstleister. Dieser überwacht auch die internen Prozessabläufe.

⁷⁶ und zwar bezüglich der für Dritte geleisteten Dienstleistungen, nicht aber des eigenen Financial Reportings.

- Controlling:

Weiterhin verfügt der Anbieter über ein internes Controlling, welches auch die Funktionsfähigkeit des Risiko-Managements überwacht.

7.3.4 Corporate Governance Codex

Der Provider unterliegt den Vorgaben des Corporate Governance Codex, den er - wie aus der Entsprechenserklärung ersichtlich - berücksichtigt. Auch dieser macht Vorgaben, insbesondere zur Rechnungslegung.

Im Rahmen der Jahresabschlussprüfung wird von den unabhängigen Wirtschaftsprüfern die Wirksamkeit des rechnungsbezogenen internen Kontroll-Systems beurteilt.

Im Falle des hier gezeigten Unternehmens hat man sich für eine SAS 70 Zertifizierung für den Betrieb des SAP-HR Systems sowie der ausgelagerten Personalabrechnung mit folgendem Umfang entschieden:

- Prüfung der Ablaufdokumentation für die Personalabrechnung inklusive der Beschreibung der durch das Unternehmen geforderten Mindestkontrollen
- Prüfung der Einhaltung der Kontrollen
- Prüfung der allgemeinen EDV-Sicherheit
- Zugriffsschutz
- Serverbetrieb
- Datensicherheit

Zunächst wird ein SAS 70 Typ I Report die sogenannte „Design Effectiveness“ aufzeigen, und in einem SAS 70 Typ II Report wird die „Control Effectiveness“ bestätigt.

Die SAS 70 Prüfung wird dann halbjährlich durch einen Wirtschaftsprüfer des Dienstleiters aktualisiert werden.

7.4 Fallbeispiel 3 - Einführung eines internen IT Kontroll-System⁷⁷

7.4.1 Gesetzliche Anforderungen und Unternehmensdarstellung

Die gesetzlichen Anforderungen werden in diesem Fallbeispiel durch KonTraG, GoBS, SOX, u.a. bestimmt. Als Referenzmodell wird CoBIT genutzt.

Zur exemplarischen Beschreibung der Herleitung eines unternehmensspezifischen Frameworks für ein internes IT-Kontroll-System auf Basis des CoBIT-Referenzmodells wurde für dieses Fallbeispiel ein Unternehmen (anonymisiert) herangezogen, das nach den Erfahrungen der Wirtschaftsprüfer sicher kein Einzelfall bei der Vorgehensweise und bei den dabei auftretenden Problemen ist. Es handelt sich um ein deutsches Technologieunternehmen im Bereich der Telekommunikation mit einer in knapp 10 Jahren rasch gewachsenen IT-Landschaft. Mittlerweile gehört das Unternehmen zu einem US-amerikanischen Konzern.

7.4.2 Ausgangslage

Die IT des Unternehmens ist eher dezentral organisiert und beschäftigt hervorragende Fachleute für die einzelnen Aufgaben und Systeme. Es gibt eine Vielzahl von selbst entwickelten Anwendungen in der IT-Systemumgebung. Die gesamte Unternehmens-IT ist über die Jahre rasant gewachsen. IT-Kontrollthemen sind eingeführt, jedoch basieren sie nicht auf einer vorgegebenen IT-Strategie oder auf einem unternehmensweiten Standard und werden in der Regel auch nicht nach vorgeschriebenen Kontrollzielen und Prüfungsplänen durchgeführt. Kontrollaufgaben werden eher aus der eigenen Erfahrung des IT-Verantwortlichen heraus wahrgenommen und nicht dokumentiert. An dieser Stelle sei vermerkt, dass die vom IT-Verantwortlichen „aus dem Bauch heraus“ durchgeführten Kontrollen meist die Richtigen sind. Sie sind aber für Zwecke der Wirtschaftsprüfung unbrauchbar, da sie nicht nachvollziehbar dokumentiert werden und meist nur auf einer Person beruhen.

In diesem speziellen Falle wurde für den Aufbau eines internen IT-Kontroll-Systems CoBIT als Modell zu Rate gezogen. Jedoch musste das Unternehmen zunächst einmal selbst in den ersten Implementierungsphasen ein Verständnis für die eigenen IT-Prozesse, deren Kontroll- und Schutzbedarf und die damit zusammenhängenden IT-Systemkomponenten schaffen. Viele der im Unternehmen bisher der Kontrolle unterlegenen IT-Bereiche hatten keinen direkten Bezug zu geschäftskritischen Anwendungen oder Prozessen und kosteten deshalb unnötig Zeit und Geld.

⁷⁷ Erläuterungen und Hilfestellungen zur Einführung eines internen IT Kontroll-Systems nach CoBIT gibt das „Praxis-handbuch COBIT: IT-Prozesse steuern, bewerten und verbessern“, Peter R. Bitterli (Hrsg.), ISBN 3-939707-007, Symposium Publishing, Düsseldorf 2006 Dieser Auszug wurde mit Genehmigung des Verlags zur Verfügung gestellt.

Andere, für die kritischsten Servicebereiche und das Financial Controlling wichtigen Bereiche wurden nur unzureichend berücksichtigt. Das vorhandene Kontroll-System in der IT richtete sich an Risiken aus, die von der IT bestimmt wurden und orientierte sich nicht an den Risiken der Unternehmensprozesse.

7.4.3 Risiko Mapping

Die Verbindung von typischen IT-Risiken⁷⁸ zu Risiken im Finanzberichtswesen, zu Prozessrisiken in der Produktion oder zu anderen Risiken sind oft nicht transparent oder nicht schlüssig abgeleitet. Teilweise fehlt eine Übersicht, welche Prozesse von welchen Anwendungen und Infrastruktur-Komponenten abhängen. Somit ist in einem ersten Schritt ein „Mapping“ aller IT-Anwendungen auf Prozessebene zu berücksichtigen.

7.4.4 Einführung interner IT-Kontrollen

Anschließend ist es bei der Entwicklung der internen IT-Kontrollen wichtig, zwischen verschiedenen Kontrollebenen zu unterscheiden. Die grundlegenden Kontrollebenen sind die sogenannten

- Entity Level Controls,
- Application Controls und die
- General Computer Controls.

Dazu muss aber ein genaues Verständnis vorliegen, welche Unternehmensbereiche (Entities), Prozesse und Anwendungen (Applications) und welche Infrastrukturkomponenten (General Computer Components) überhaupt betroffen sind.

In diesem Praxisbeispiel war es von herausragender Bedeutung, die Limitationen der bestehenden IT zu verstehen. Gerade bei historisch gewachsenen Systemen mit bekannten Schwachstellen ist es entscheidend, in einem Kontroll-System nicht nur die vielleicht theoretisch und vom CoBIT-Referenzmodell vorgegebenen Kontrollziele und –aufgaben einzubeziehen, sondern sich bestehender Schwächen bewusst zu sein, sich auf die von der Unternehmensführung festgelegten Risiken und geschäftskritischen Prozesse zu konzentrieren und dann auch bewusst einige Themenbereiche aus dem Kontroll-System herauszulassen. Ein stringent nach einem Standard aufgesetztes Kontroll-System erfährt zu dem auch keine Unterstützung bei den verantwortlichen Mitarbeitern.

Bei der Durchführung von internen Kontrollen und der Anpassung eines Kontroll-Systems auf ganz spezielle, unternehmensspezifische Belange werden vor allem im Nachhinein noch eine

⁷⁸ zum Beispiel der IT-Infrastruktur.

Anzahl von Fragestellungen aufgeworfen, die soweit es geht schon bei der Entwicklung des Kontroll-Systems berücksichtigt werden können.

7.4.5 Fragen bei der Einführung eines internen IT-Kontroll-Systems nach CoBIT

- In welcher Ausführlichkeit und Detailtreue müssen die Kontrollen dokumentiert werden?
- Welche Anzahl von Stichproben reicht aus, um aussagekräftige Prüfaussagen zu erhalten?
- Wann müssen spezifische Anwendungskontrollen zum Beispiel bei Änderungen in der Anwendung oder Software-Updates mit in das interne Kontroll-System einbezogen werden?
- Nach welchem Verfahren werden Kontrollaktivitäten geändert, sofern sich einige der Kontrollen als unwirksam herausstellen?
- Nach welchen Kriterien müssen Kontrollfeststellungen bewertet werden? Gibt es hierzu die Notwendigkeit für festgelegte Eskalationsstufen?
- Wie können Änderungen in den Prozessstrukturen oder der Risikostruktur später problemlos in das Kontroll-System einbezogen werden?

7.5 Fallbeispiel 4 - Auslagerung eines Rechenzentrums

Die Firma Streck GmbH entscheidet sich für ein Outsourcing des Rechenzentrums an die Firma RYLE Ltd in China. Die Firma RYLE hat keine eigene Entscheidungsbefugnis. Sie hat keine (vertragliche) Beziehung zu den von der Datenverarbeitung Betroffenen, und sie hat nur Umgang mit Daten, die der Auftraggeber ihr zur Verfügung stellt. Verbindliche Unternehmensregelungen bestehen nicht.

Bei dem Outsourcing handelt es sich um eine Auftragsdatenverarbeitung. Da die Datenübermittlung und -verarbeitung außerhalb Europas stattfindet, muss sichergestellt werden, dass das europäische Datenschutzniveau eingehalten wird. Verantwortlich hierfür ist die Streck GmbH. Ein Safe-Harbor-Abkommen gilt nur für die Vereinigten Staaten. China zählt nicht zu den Ländern, zu denen die Europäische Kommission bereits entschieden hat, dass ein angemessenes Datenschutzniveau herrscht. Da verbindliche Unternehmensregelungen nicht bestehen, bleibt der Firma Streck GmbH die Möglichkeit, im Rahmen der Auftragsdatenverarbeitung die EU-Standardvertragsklauseln anzuwenden. Die Einhaltung des europäischen Datenschutzniveaus ist somit gesichert. Durch die Anwendung der EU-Standardvertragsklauseln kommt es darüber hinaus zu einer analogen Anwendung des § 3 Abs. 8 Satz 3 BDSG, so dass eine weitere Einwilligung der Betroffenen nicht notwendig ist.

8 Glossar

Nachfolgend bedeuten: S: Synonym, K: Kontext, O: Oberbegriff, M: Metabegriff

Begriff	Beschreibung
Application Hosting	<p>Beim Application Hosting geht die Betriebsverantwortung für Anwendungen an einen externen Dienstleister über. Im Gegensatz zum Application Outsourcing findet i.d.R. kein Personal- und Assetübergang statt (vgl. →Personnel Transfer und →Asset Transfer). Ebenso verbleiben die Anwendungslizenzen im Gegensatz zum →ASP-Modell i.d.R. im Eigentum des Kunden (vgl. auch →Beistellung).</p> <p>S: -, K: Application Outsourcing, O: Application Outsourcing , M: Dienstleistung</p>
Application Outsourcing	<p>Form des IT-Outsourcing, bei der die Verantwortung für die sachgerechte Funktionsfähigkeit der Anwendung auf einen externen Dienstleister übergeht. Der Dienstleister erbringt auf Basis fest definierter →SLA's sämtliche Leistungen wie z.B. Software-Entwicklung, Implementierung, Erweiterung, Support, Migration und Betrieb der Anwendung. Infrastruktur und Software-Lizenzen können ebenfalls übertragen werden. In vielen Fällen werden Lizenzen aber in Form einer →Beistellung vom Kunden zur Verfügung gestellt. Beim Application Outsourcing findet oft eine →Mitarbeiterübernahme statt.</p> <p>S: -, K: IT-Outsourcing, O: IT-Outsourcing, M: Dienstleistung</p>
Application Service Provision	<p>Eine Spezialform des →Application Outsourcing bei der i.d.R. browser-/internetfähige Applikationen auf Basis eines nutzungsabhängigen Miet-Modells über ein Wide-Area-Network (WAN) - i.d.R. das World-Wide-Web - vom Rechenzentrum des Application Service Provider aus zur Verfügung gestellt werden. Es wird unterschieden:</p> <ol style="list-style-type: none"> 1. Emulations-ASP: Der Nutzer greift über ein browserfähiges Terminal und über eine verschlüsselte Internetverbindung auf die Anwendungen zu, die auf dem Server des ASP-Anbieters ablaufen. 2. Applet-ASP: dem Nutzer werden einzelne Applets auf seinem Computersystem zur Verfügung gestellt; das eigentliche (betriebs-systemgebundene) Programm verbleibt hingegen beim Application Service Provider. 3. Wartungs-ASP: Erscheinungsform des ASP, bei der das betreffende Computerprogramm auf dem Rechner des Nutzers abläuft und lediglich die Wartung des Programms auf den Anbieter verlagert wird.

Begriff	Beschreibung
	S: Application Service Providing, K: Application Outsourcing, O: Application Outsourcing, M: Dienstleistung
Asset Deal	Kaufgegenstand bei einem Asset Deal im Rahmen eines (IT-)Outsourcing-Projektes sind die materiellen und immateriellen Wirtschaftsgüter einer (IT-)Organisation oder eines (IT-)Unternehmens. Vgl. auch →Asset Transfer. Im Gegensatz vgl. auch: →Share Deal. S: -, K: Vertrag, O: -, M: Vertragskomponente
Asset Transfer	Übergang von Vermögenswerten (=Assets: z.B. (IT-)Betriebsmitteln wie Hard-/Software, Prozesse, Know-how) und/oder Gebäuden (Rechenzentren) vom Kunden in das Eigentum des Outsourcing-Dienstleisters. In den meisten Fällen werden die Betriebsmittel zum Restbuchwert oder zum fairen Marktwert („fair market value“) übernommen. Asset-Transfer führt zu einer Reduzierung des Anlagevermögens beim Kunden. Die Übertragung geschieht juristisch bei beweglichen Sachen (z.B. Hardware) durch Übereignung gem. § 929 BGB, bei Immaterialgüterrechten durch Abtretung gem. § 398 BGB sowie durch Lizenzierung bei Verträgen durch Vertragsübernahme gem. § 305 BGB. S: Asset Takeover; Asset-Übernahme, K: Vertrag, O: -, M: Vertragskomponente
Balanced Scorecard	Eine Technik der Leistungsmessung, die zur Unternehmensführung eingesetzt wird, um verschiedene interne Funktionen und deren Ergebnisse nach außen zu messen. Mit der Balanced Scorecard steuern Organisationen das Erreichen von strategischen Zielen, die oft in vier Felder eingeteilt sind (Finanzen, Prozesse, Kunden/Markt, Personal). Die Ziele werden durch KPI gemessen, die auf die Strategie abgestimmt sind.
Base Case (Baseline)	Ermittlung der aktuellen und tatsächlich existierenden (Kosten)Situation des Kunden, ergänzt um eine Projektion der bei einem Eigenbetrieb zukünftig zu erwartenden Kostenentwicklung. Mittels Base Case lässt sich ein realistischer Vergleich zu den Outsourcing-Angeboten externer Dienstleister herstellen (vgl auch: →Due Diligence). S: Base Line, K: Outsourcing-Prozess, O: -, M: Zustand
Beistellung	Eigentumswerte (Assets), die im Eigentum des Kunden verbleiben, können einem Outsourcing-Provider im Rahmen der Vertragserfüllung zum Gebrauch überlassen (beigestellt) werden. Dies geschieht häufig bei Softwarelizenzen, um die Notwendigkeit einer Neulizensierung zu vermeiden. S: -, K: Vertrag, O: -, M: Vertragskomponente

Begriff	Beschreibung
Betriebs- übergang	<p>Wird beim Abschluss eines Outsourcing-Vertrages ein Betrieb oder Betriebsteil auf den Dienstleister übertragen, so gehen auch die zu dieser Zeit bestehenden Arbeitsverhältnisse der in diesem Betrieb(steil) beschäftigten Arbeitnehmer auf den neuen Inhaber über (vgl. auch: →Personnel Transfer). Er tritt dann in die Rechte und Pflichten aus diesen Arbeitsverhältnissen ein.</p> <p>S: -, K: Vertrag, O: -, M: rechtliche Rahmenbedingung</p>
Business Innovation Partner	<p>Als 'Business Innovation Partner' bezeichnet man eine neue Kategorie von Dienstleistern im Markt der Beratungs- und IT-Dienstleistungen. Ihre zentralen Kriterien sind ganzheitliche Beratungs- und Integrationsdienstleistungen, Veränderung von Geschäftsprozessen, Partnerschaftlichkeit und Mitverantwortung.</p> <p>S: -, K: Dienstleister, O: Dienstleister, M: Dienstleister</p>
Business Process Outsourcing	<p>Outsourcing eines kompletten Geschäftsprozesses oder Teilen davon und ggf. der dazu erforderlichen – den Prozess unterstützenden - IT-Infrastruktur durch einen externen Dienstleister. Im diesem Zusammenhang gehen i.d.R. auch Personal und Assets auf den Dienstleister über. Folgende Geschäftsprozesse werden z.B. als auslagerungsfähig angesehen:</p> <ul style="list-style-type: none"> ■ Personalwesen (Payroll), ■ Beschaffung, ■ Finanzwesen/Buchhaltung (Accounts Receivables), ■ Logistik (SCM), ■ Ausbildung/Training (e-Learning) <p>Im Gegensatz zum →Business Transformation Outsourcing (BTO) erfolgt i.d.R kein Re-engineering der Prozesse</p> <p>S: -, K: IT-Outsourcing, O: IT-Outsourcing, M: Dienstleistung</p>
Business Transformation Outsourcing	<p>Hierbei handelt es sich um die wirtschaftliche Verknüpfung zweier paralleler Outsourcing-Projekte: Dem Re-Engineering und dem Betrieb von Geschäftsprozessen (inkl. der notwendigen Neuentwicklung oder Überführung der bestehenden Anwendungen auf eine neue technische Plattform) und dem Betrieb der IT-Infrastruktur. Damit übernimmt der externe Dienstleister beim BTO die Betriebsverantwortung für einen ganzen Geschäftsprozess mit dem Ziel einer Transformation und kontinuierlichen Optimierung.</p> <p>Das „Transformierende Outsourcing“ verändert die Geschäfte des Kunden am gründlichsten, insbesondere dann, wenn dadurch Innovationen und</p>

Begriff	Beschreibung
	<p>neue Geschäfts-Modelle eingeführt werden.</p> <p>S: -, K: IT-Outsourcing, O: IT-Outsourcing, M: Dienstleistung</p>
Business Case	<p>Erweiterte Wirtschaftlichkeitsberechnung; in der Regel über mehrere Jahre. Es werden diskontierte Aufwände und Erträge oder vereinfacht operative Einsparungen gegen Investitionen gegenübergestellt, die mit dem BPO ursächlich verbunden sind (z.B. Senkung des Personalaufwands, Senkung des Sachaufwandes). Zurechenbare Umsatzerhöhungen, etwa durch verbesserte Prozesse, können ebenfalls berücksichtigt werden. Neben der reinen Finanzanalyse enthält der Business Case die Beschreibung der Rahmenbedingungen und in der Regel eine Analyse und Bewertung der Risiken.</p>
Business Performance Transformation Services	<p>Business Performance Transformation Services (BPTS) zielen auf eine umfassende Verbesserung der bestehenden Geschäftsprozesse, aber auch darauf, innovative Wege für das Business zu entwickeln. Oft begleitet durch eine Transformation mit dem Ziel Geschäfts-Modelle, Prozesse und Systeme effektiver, effizienter und wettbewerbsfähiger zu gestalten. Ein Beispiel ist die Frage nach der notwendigen Spezialisierung, um das Geschäfts-Modell optimal (auch im Netzwerk mit Kunden, Lieferanten, Partnern und Mitarbeitern) zu unterstützen. Ausprägungen sind u.a.: Shared Service Center (interne Spezialisierung) oder BTO (externe Spezialisierung).</p>
Change Management	<p>Standardisierte Prozesse und Verfahren, die dazu dienen, Änderungen eines definierten Leistungsumfangs zu analysieren, zu entwerfen, vertraglich zu fixieren und zu realisieren.</p> <p>S: -, K: Service-Management, O: -, M: Prozess</p>
Change Request	<p>Anforderung bzgl. einer Modifikation der vereinbarten Leistungsinhalte (→Service-Level Agreements), weil z.B. die Veränderung von Mengengerüsten eine Anpassung der bereitzustellenden Ressourcen erfordert.</p> <p>S: -, K: Service-Management, O: -, M: Dokument</p>
Commodity	<p>Ein „gewöhnlicher“ Outsourcing-Service, der von einer Vielzahl von Anbietern in vergleichbarer Qualität erbracht werden kann und damit relativ leicht einen Anbieterwechsel möglich macht. Als Commodity wird heute häufig z.B. der Betrieb von Rechenzentren angesehen.</p> <p>S: -, K: Marketing, O: -, M: Marketingbegriff</p>
Co-Sourcing	<p>Mitarbeiter des Outsourcing-Dienstleisters übernehmen auf Zeit Schlüssel-/Führungspositionen in der Organisation des Kunden und führen beispielsweise gemeinsam mit der Kundenorganisation eine Konsolidie-</p>

Begriff	Beschreibung
	<p>rung / Reorganisation / Transformation der IT- /Prozess-Umgebung durch. Nach erfolgter Transformation geht die Verantwortung wieder vollständig auf den Kunden über. Ein →Transfer von Personal und →Assets findet bei diesem Modell nicht statt.</p> <p>Die Bezahlung des Outsourcing-Dienstleisters erfolgt i.d.R. nach dem messbaren Erfolg der Reorganisation.</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>
Data Center Outsourcing	<p>Outsourcing des zentralen Rechenzentrums. Teil des →Infrastructure Outsourcing. Ein Rechenzentrum beinhaltet i.d.R. die zentralen Server und zugehörigen Systemkomponenten (z.B. Speichersysteme, Softwarekomponenten, Kommunikationseinrichtungen). Es ist die physische und organisatorische Einheit, die zentrale IT-Leistungen wie Beratung, Planung, Beschaffung, Installation, Betrieb und weitere Services erbringt und damit IT-Infrastrukturkapazitäten für ein Unternehmen bereitstellt.</p> <p>S: Rechenzentrums-Outsourcing, K: Infrastructure Outsourcing, O: Infrastructure Outsourcing, M: Dienstleistung</p>
Delivery	<p>Projektphase des laufenden Betriebes auf Basis der Bedingungen des Outsourcing-Vertrages und insbesondere der dort festgeschriebenen →Service-Level-Agreements (SLA's) über die vereinbarte Vertragslaufzeit.</p> <p>S: Service Delivery, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Delivery Center	<p>Physische Lokation, aus der heraus der Outsourcing-Dienstleister seine Services erbringt.</p> <p>S: -, K: Lösung, O: -, M: Lösungskomponente</p>
Desktop Outsourcing	<p>Ist ein Service im Rahmen des →Infrastructure Outsourcing. Zusammenfassender Begriff für die Outsourcing-Dienstleistungen, die sich auf die am Arbeitsplatz des Endbenutzers befindlichen Systemkomponenten – die dezentrale IT-Infrastruktur - beziehen. Das typische Leistungsspektrum umfaßt Betrieb, Installation, Wartung und Lieferung der Endbenutzer-IT (→IMAC: Installation, Moves, Adds, and Changes) durch den Outsourcing-Provider.</p> <p>S: Workplace Services, K: Infrastructure Outsourcing, O: Infrastructure Outsourcing, M: Dienstleistung</p>
Due Diligence	<p>Umfassende, auch körperliche (physische) Bestandsaufnahme und Bewertung der beim Kunden vorhandenen und vom Outsourcing betroffenen (IT-)Infrastruktur, deren Managementprozesse und Rahmenbedingungen.</p> <p>Ziel ist, möglichst umfassende Informationen über die Betriebsumgebung</p>

Begriff	Beschreibung
	<p>zu gewinnen. Diese Informationen dienen dazu, alle relevanten technischen, rechtlichen und betriebswirtschaftlichen Aspekte in das Outsourcing-Angebot oder ggf. in das Angebot einer Betriebsübernahme (vgl. auch: →Share Deal und →Asset Deal) einzubeziehen. Im Falle der Personalübernahme (vgl. auch →Personnel Transfer) empfiehlt sich auch eine Human Resource Due Diligence durchzuführen.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Entlastungsstrategie	<p>Als Entlastungsstrategie wird eine Sourcing-Strategie (→Sourcing, →Sourcing Strategy) bezeichnet, die lediglich operative Prozesse oder Funktionen schneller und kostengünstiger - also effizienter – gestalten will. Bei der Entlastungsstrategie werden periphere Tätigkeiten verlagert, die nicht direkt zu den Hauptaufgaben des Unternehmens gehören. Im Gegensatz dazu verfolgt eine →Erweiterungsstrategie strategische Ziele.</p> <p>S: , K: , O: Sourcing-Strategie, M:</p>
Erweiterungsstrategie	<p>Die Erweiterungsstrategie konzentriert sich – im Unterschied zur →Entlastungsstrategie - auf die Erhöhung der Wertschöpfung von Unternehmen bei Konzentration auf deren Kernkompetenzen.</p> <p>S: , K: , O: Sourcing-Strategie, M:</p>
Fertigungstiefe	<p>Fertigungstiefe⁷⁹ ist der Anteil der Fertigungsprozesse, die vom Endhersteller selbst durchgeführt werden.</p> <p>Eine Fertigungstiefe von Null bedeutet, dass das Unternehmen keine eigene Produktion oder Veredelung von Produkten hat, sich also allein auf den Handel beschränkt. ... Eine Fertigungstiefe von 100% würde bedeuten, dass das Unternehmen ohne jeglichen Zukauf von Komponenten oder Rohstoffen in vollständiger Autarkie Produkte herstellt.</p> <p>Beispielsweise wird aus Erz über mehrere Fertigungsstufen eine Nockenwelle oder ein Kochtopf.</p> <p>Aus ökonomischen Gründen hat die Fertigungstiefe ein Optimum. Die Fertigungstiefe ist ein wesentlicher Indikator der Programmtiefe.</p> <p>S: , K: , O: , M:</p>

⁷⁹ <http://de.wikipedia.org/wiki/Fertigungstiefe>.

Begriff	Beschreibung
Full Scope Outsourcing	Vgl. auch →Total (IT-) Outsourcing S: Total Outsourcing; Total IT-Outsourcing, K: Outsourcing, O: Outsourcing, M: Strategie
Gain Sharing	Vertraglich festgelegter Erfolgsbeitrag des Dienstleisters zur Geschäftstätigkeit des Kunden auf Basis einer leistungsabhängigen Entlohnung des Dienstleisters (Vgl. →Risk and Reward Sharing). Gain Sharing Verträge setzen voraus, dass die Leistungsindikatoren des Dienstleisters mit den betrieblichen Kennzahlen des Kunden verknüpft werden können. Das Modell erfordert im Wesentlichen folgendes Vorgehen: <ul style="list-style-type: none"> ■ Definition und Auswahl der betrieblichen Kennzahlen ■ Benchmarking dieser Kennzahlen ■ Entwicklung von Leistungsindikatoren (Key Performance Indicators – KPI) ■ Entwurf des Gain Sharing Vertrags ■ Financial Engineering ■ Leistungsbereitstellung turnusmäßige Überprüfung und Anpassung der Kennzahlen ■ Überprüfung von Investitionsalternativen S: Risk and Reward Sharing, K: Pricing, O: -, M: Preis-Modell
Governance (Model)	Organisatorische partnerschaftliche Konzeption zur Sicherstellung einer vertrauensvollen Kooperation zwischen Kunde und (IT-)Dienstleister im Rahmen einer Outsourcing-Beziehung. S: Outsourcing Governance Model, K: Service-Management, O: -, M: Prozess
Hosting	Sammelbezeichnung für alle Leistungen, welche die physische Auslagerung von IT-Ressourcen betreffen. Dazu zählen unter anderem Rechenzentrumsleistungen, Web-Hosting (Betrieb von Web-Sites und Online-Anwendung auf den Servern des Anbieters), Co-Location, und Managed-Hosting sowie System Disaster Recovery Services. Beispiele: <ol style="list-style-type: none"> 1. Möglichkeit, einen eigenen Computer oder einen virtuellen Server bei einem Outsourcing-Provider in eigener Verantwortung zu betreiben (vgl. auch →Co-Location Services). 2. Bereitstellen von Web-Space auf einem externen Server des Hosting-Anbieters, um Web-Seiten, Programme oder Anwendungen im Internet zugänglich zu machen. Oft wird dafür auch der Begriff →Web Hosting verwendet. Im Gegensatz zum Outsourcing ist in reinen Hosting-Verträgen in der

Begriff	Beschreibung
	<p>Regel keine Personal- oder Asset-Übernahme vorgesehen (vgl. →Personnel Transfer und →Asset Transfer); auch ist die Vertragslaufzeit aufgrund der geringeren Komplexität und des geringeren Investitionsvolumens i.d.R. kürzer.</p> <p>S: Housing, K: Infrastructure Outsourcing, O: Infrastructure Outsourcing, M: Dienstleistung</p>
Infrastructure Outsourcing	<p>Teil des →IT-Outsourcing, bei dem Betrieb und Wartung der Infrastruktur bzw. von Teilen der IT-Infrastruktur sowie Support-Dienstleistungen durch einen externen Dienstleister vollverantwortlich erbracht werden. Dem Infrastruktur-Outsourcing werden i.d.R. folgende IT-Felder zugeordnet:</p> <ul style="list-style-type: none"> ■ Rechenzentrum (Host/Zentrale Server) →Data Center Outsourcing, ■ Netze (Local Area Network, Wide Area Network) →Network Outsourcing ■ Arbeitsplatzsysteme (Desktop Services) →Desktop Outsourcing ■ Endbenutzer Support (→User Help Desk) ■ Anderes (z.B. Security-Aufgaben, Druckstrassen, Telefonsysteme) →Security Outsourcing <p>S: Infrastruktur-Outsourcing, K: IT-Outsourcing, O: IT-Outsourcing, M: Dienstleistung</p>
Insourcer	<p>Der Begriff wird mehrdeutig verwendet:</p> <ul style="list-style-type: none"> ■ Organisationseinheit eines Unternehmens, die im Rahmen eines „Shared Service Centers“ (IT-)Leistungen für unternehmensinterne Abteilungen/Bereiche erbringt. ■ Organisationen, die durch die Überführung (Ausgründung) einer ehemaligen (IT-)Abteilung eines Unternehmens in eine rechtlich selbständige Tochtergesellschaft („(IT-)GmbH“) entstanden sind. Diese (IT-)Töchter versorgen i.d.R. den jeweiligen Mutterkonzern mit (IT-)Services auf der Basis quasi-formaler Verträge und Service-Level-Agreements und werden üblicherweise an ihrem eigenen Erfolgsbeitrag (profit and loss) gemessen. Häufig erfolgen diese Ausgründungen auch mit der Zielsetzung, ihre Dienstleistungen auf dem freien Markt anzubieten. <p>S: Interner Outsourcer, K: Dienstleister, O: -, M: Dienstleister</p>
Insourcing	<p>Der Begriff wird mehrdeutig verwendet:</p> <ol style="list-style-type: none"> 1. Eigenbetrieb der IT 2. Rückübernahme eines ehemals ausgelagerten (IT-)Betriebes in die eigene Organisation nach Ablauf eines Outsourcing-Vertrages oder bei

Begriff	Beschreibung
	<p>dessen vorzeitiger Beendigung (Rückabwicklung).</p> <p>3. Ausgründung der (IT-)Abteilung eines Unternehmens in eine rechtlich selbständige Tochtergesellschaft (→Insourcer)</p> <p>S: Backsourcing; →Rückabwicklung; Internes Outsourcing, K: Sourcing, O: Sourcing, M: Strategie</p>
IT-Outsourcing	<p>Information Technology (IT) Outsourcing ist die vollverantwortliche Übertragung von IT-Funktionen oder Geschäftsprozessen mit hohem IT-Anteil an rechtlich selbständige - d.h. externe – Dienstleister über einen definierten Zeitraum. Dabei gehen häufig Assets und Personal auf den Dienstleister über. Die Qualität der vertraglich definierten Leistung wird durch Service-Level Agreements (SLA) beschrieben.</p> <p>IT-Outsourcing umfasst folgende Dimensionen:</p> <p>Nach der Leistungsebene („was“):</p> <ol style="list-style-type: none"> 1. Infrastrukturebene (→Infrastructure Outsourcing) 2. Anwendungsebene (→Application Outsourcing) 3. Geschäftsprozessebene (→Business Process Outsourcing) <p>Nach dem Umfang (“wie viel“):</p> <ol style="list-style-type: none"> 1. Teile von Funktionen//Prozessen (Selective Outsourcing) 2. Komplette Funktionen/Prozesse (Full Scope Outsourcing) <p>Nach der Anzahl der Dienstleister (“wer”)</p> <ol style="list-style-type: none"> 1. ein Dienstleister (Single Vendor Outsourcing) 2. mehrere Dienstleister (Multi Vendor Outsourcing) <p>Nach dem Ort der Leistungserstellung (“woher”)</p> <ol style="list-style-type: none"> 1. im Land (Onshore Outsourcing) 2. im näheren Ausland (Nearshore Outsourcing) 3. in Übersee (Offshore Outsourcing) <p>Nach Dienstleistungsempfänger (“für wen”)</p> <ol style="list-style-type: none"> 1. für einzelne Organisationseinheiten 2. für die gesamte Organisation <p>Nach dem Ort der Dienstnehmer (“wohin”)</p> <ol style="list-style-type: none"> 1. weltweit (Global Outsourcing) 2. regional (Regional Outsourcing) 3. national (National Outsourcing) 4. lokal (Local Outsourcing)

Begriff	Beschreibung
	<p>Ist ein Re-Engineering der übertragenen Funktionen oder Prozesse wesentlicher Bestandteil von IT-Outsourcing, spricht man von (→Business Transformation Outsourcing).</p> <p>S: -, K: Outsourcing, O: Outsourcing, M: Dienstleistung</p>
Joint Venture	<p>Im Rahmen eines Outsourcing-Vorhabens von Kunde und →Outsourcing-Provider gegründetes Gemeinschaftsunternehmen mit dem Zweck, (IT-)Dienstleistungen für die Gesellschafter und/oder für Dritte zu erbringen. In den meisten Fällen liegt die Mehrheit der Geschäftsanteile bzw. die unternehmerische Führerschaft beim Outsourcing-Dienstleister.</p> <p>S: Gemeinschaftsunternehmen, K: Lösung, O: -, M:</p>
Komplettes IT-Outsourcing	<p>Vgl. →Total Outsourcing.</p> <p>S: Total Outsourcing; Full Scope Outsourcing; Full Outsourcing; One-stop-shopping, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Last Call Option	<p>Die finale Möglichkeit für einen Outsourcing-Anbieter die offengelegten Preise der Mitbewerber zu unterbieten. Diese Option wird i.d.R. dem →Provider, zu dem bereits Vertragsbeziehungen bestehen oder der eigenen (IT-)Organisation (→Insourcer) eingeräumt.</p> <p>S: -, K: -, O: -, M:</p>
Leistungstiefe	<p>Die Leistungstiefe⁸⁰ ist der Anteil an den eigenen Verwaltungs- bzw. administrativen Aufgaben eines Unternehmens, welcher durch das Unternehmen selber ausgeführt wird.</p> <p>So wie in der herstellenden Industrie über die →Fertigungstiefe der eigene Anteil zur Herstellung eines Produkts bezeichnet wird, handelt es sich bei der Leistungstiefe um den Anteil der eigenen Verwaltungs- bzw. administrativen Aktivitäten. Wird z.B. die Buchhaltung in kleineren Betrieben durch einen Steuerberater geleistet bzw. in größeren Betrieben an einen Dienstleister outsourced, reduziert sich die Leistungstiefe des Unternehmens. Es wird erwartet, dass durch das so genannte →Business Prozess Outsourcing (BPO) sich die Leistungstiefe in den nächsten Jahren wesentlich reduzieren wird. Motive, so vorzugehen, können entweder in einer →Entlastungsstrategie oder einer →Erweiterungsstrategie liegen.</p> <p>S: , K: , O: , M:</p>

⁸⁰ <http://de.wikipedia.org/wiki/Leistungstiefe>.

Begriff	Beschreibung
Managed Service	<p>Oberbegriff für alle auf die IT-Infrastruktur bezogenen externen Dienstleistungen, die i.d.R. remote erbracht werden. Bei Managed Service erfolgt im Gegensatz zum Outsourcing kein →Personal- und/oder →Asset-Transfer. Managed Services können z.B. für Netze, Sicherheitseinrichtungen, Datenbanken, Server, Speichersysteme und Anwendungen erbracht werden.</p> <p>S: →Outtasking, K: Outsourcing, O: Dienstleistung, M: Dienstleistung</p>
Master Agreement	<p>Im internationalen Bereich gebräuchliche Bezeichnung für einen internationalen Outsourcing-Rahmenvertrag, an dem sich dann die jeweiligen nationalen Vereinbarungen (National Agreements) inhaltlich orientieren.</p> <p>S: Framework Agreement, K: Vertrag, O: -, M: Vertragskomponente</p>
Mitarbeiterübernahme	<p>Siehe auch →Personnel Transfer</p> <p>S: Personnel Transfer; Personnel Takeover; Personalübergang, K: Vertrag, O: -, M: Vertragskomponente</p>
Multi Vendor Outsourcing	<p>Verschiedene (IT-)Aufgaben werden im Rahmen einer →Selective Outsourcing-Entscheidung an mehrere Anbieter vergeben (vgl. auch im Gegensatz dazu: →Single Vendor Outsourcing). Die Vorteile dieser Form des Outsourcing liegen darin, dass für jeden Teilbereich ein Spezialist zuständig ist. Komplex ist dagegen die tatsächliche und rechtliche Bewältigung der Schnittstellen und das tägliche Management der einzelnen Anbieter.</p> <p>S: Multi Sourcing, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Nearshore Outsourcing	<p>Die Outsourcing-Leistungen werden – z.B. von Deutschland aus gesehen - in europäischen bzw. europahanen Standortorten erbracht. Wesentliche Kennzeichen sind ein geringes Lohnniveau, sprachliche bzw. kulturellen Affinitäten und relative geopolitische Nähe. Die Erbringung folgender (IT-)Dienstleistungen ist dabei möglich:</p> <ul style="list-style-type: none"> →Infrastructure Outsourcing →Application Outsourcing →Business Process Outsourcing →Business Tranformation Outsourcing <p>S: -, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Nearshoring	<p>Die Leistungen werden – z.B. von Deutschland aus gesehen -in europäischen bzw. europahanen Standortorten erbracht. Wesentliche Kennzeichen sind ein geringes Lohnniveau, sprachliche bzw. kulturellen Affinitäten und relative geopolitische Nähe.</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>

Begriff	Beschreibung
Offshore Outsourcing	<p>Erbringen von Outsourcing-Services durch einen Dienstleister aus einem Standort mit viel geringerem Lohnniveau (oft Asien). Dem Vorteil des sehr viel niedrigen Kostenniveaus stehen teilweise Risiken aufgrund sprachlicher, kultureller und geopolitischer Strukturen gegenüber.</p> <p>Die Erbringung folgender Dienstleistungen ist im Offshore Outsourcing möglich:</p> <ul style="list-style-type: none"> →Infrastructure Outsourcing →Application Outsourcing →Business Process Outsourcing →Business Transformation Outsourcing <p>S: Offshore Sourcing; Farshoring, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Offshoring	<p>Erbringen von Leistungen durch Unternehmen von außereuropäischen – oft asiatischen - Standorten. Dem Vorteil eines sehr viel geringeren Lohnniveaus stehen teilweise Risiken aufgrund sprachlicher, kultureller, geopolitischer Strukturen gegenüber.</p> <p>S: Farshoring; Farshore Sourcing, K: Sourcing, O: Sourcing, M: Strategie</p>
On-Demand Outsourcing	<p>Wird häufig als Outsourcing-Preis-Modell gesehen. Solche Modelle beschreiben Pricing- und Delivery-Modelle für Outsourcing-Services auf Basis von Bedarf und Verbrauch. Die Grundidee ist, dass der Kunde nur noch für die (IT-)Leistungen bezahlt, die er auch tatsächlich verbraucht hat. Die (IT-)Kosten passen sich damit flexibel dem Geschäftsverlauf an; eine Vorratshaltung von (IT-)Kapazitäten wird überflüssig.</p> <p>S: Utility Outsourcing, K: Pricing, O: -, M: Preis-Modell</p>
Onshore Outsourcing	<p>Beim Onshore Outsourcing erbringt der externe Dienstleister die Leistungen im gleichen Land, in dem sich die Abnehmer befinden. Sprachliche und kulturelle Risiken sind nicht zu erwarten. Die Kostenreduktion wird durch Skaleneffekte beim Anbieter erreicht.</p> <p>Die Erbringung folgender Dienstleistungen ist dabei möglich:</p> <ul style="list-style-type: none"> →Infrastructure Outsourcing →Application Outsourcing →Business Process Outsourcing →Business Transformation Outsourcing <p>S: -, K: Outsourcing, O: Outsourcing, M: Strategie</p>

Begriff	Beschreibung
Onshoring	<p>Die Leistungen werden aus dem Land heraus erbracht, in dem auch die Dienstnehmer lokalisiert sind. Wesentliche Kennzeichen sind gleiches oder ähnliches Lohnniveau, sprachliche bzw. kulturellen Identität und enge geopolitische Nähe.</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>
Outsourcing	<p>Allgemeiner Oberbegriff für die vollverantwortliche Übertragung betrieblicher Funktionen an rechtlich selbständige - d.h. externe - Dienstleister über einen definierten Zeitraum. Motive für Outsourcing sind z.B. Kostenreduktion, Verbesserung der Qualität und Zugriff auf Spezialwissen. Outsourcing-fähig sind Felder, die nicht zur Kernkompetenz eines Unternehmens zählen, wie z.B. Fuhrpark, Kantine oder auch die Informationstechnologie (IT). Im letzteren Fall spricht man von →IT-Outsourcing</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>
Outtasking	<p>Der Begriff wird mehrdeutig verwendet:</p> <ol style="list-style-type: none"> Übertragung von (IT-)Teilaufgaben (z.B. des Infrastruktur- oder Applikationsbetriebs) an einen externen Dienstleister, i.d.R. ohne →Personal- und →Asset-Übergang. Die beim →IT-Outsourcing oft kritisierte hohe Abhängigkeit vom Provider wird verringert, da nicht alle Aufgaben, Verantwortungen und Kompetenzen nach aussen bzw. an einen einzigen Partner übertragen werden. →Selective Outsourcing. Im Unterschied zum Outtasking kann hier häufiger ein Asset- und Personalübergang stattfinden. <p>S: Task sourcing, K: Sourcing, O: Sourcing, M: Strategie</p>
Partielles Outsourcing	<p>Vgl.: →Selective Outsourcing</p> <p>S: Selektives Outsourcing; Smart Outsourcing; Smart Sourcing; Best of Breed Outsourcing, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Personnel Transfer	<p>Mit der Verlagerung der (IT-)Aufgaben (Betriebsübergang) findet häufig auch ein Personalübergang vom Kunden auf den Outsourcing-Dienstleister statt.</p> <p>Dieser erfolgt nach den in dem jeweiligen Land geltenden gesetzlichen Regelungen. In Deutschland nach § 613 a BGB; vergleichbaren Schutz - mit landesspezifischen Varianten - gibt es auch in den anderen europäischen Ländern oder als EU-Recht unter dem Kürzel TUPE.</p> <p>S: Personalübergang; Personnel Takeover; Mitarbeiter-übernahme, K: Vertrag, O: -, M: Vertragskomponente</p>

Begriff	Beschreibung
Problem Management	<p>Prozess für die Behandlung, Lösung und Vermeidung von Störungen in der operativen Systemumgebung. Im Unterschied zum Incident Management, wo Störungen kurzfristig behoben werden, befasst sich das Problem Management mit der grundsätzlichen und langfristigen Beseitigung des Problems (root-cause-analysis).</p> <p>S: Service-Management, K: -, O: -, M: Prozess</p>
Processing Services	<p>IT-Verarbeitung von hochstandardisierten, oft durch gesetzliche Regelungen normierten, Geschäftsprozessen durch einen externen Dienstleister i.d.R. für eine Vielzahl von Kunden.</p> <p>Beispiele: Lohn-/Gehaltsabrechnung („Payroll-Services“), Kreditkartenabrechnung.</p> <p>S: -, K: Application Outsourcing, O: Application Outsourcing, M: Dienstleistung</p>
Request for Information (RFI)	<p>Aufforderung eines Kunden an einen Outsourcing-Anbieter, im Rahmen einer geplanten Ausschreibung einen Fragenkatalog zu bearbeiten, der i.d.R. Fragen zum Unternehmen des Anbieters aber auch eine Skizze des beabsichtigten Outsourcing-Vorhabens enthält. Das RFI dient zur Vorauswahl derjenigen Anbieter, die in die Ausschreibung einbezogen werden und dann das →RFP erhalten.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Request for Proposal (RFP)	<p>Angebotsaufforderung, der häufig ein →RFI vorausgeht. Das RFP enthält i.d.R. eine ausführliche Beschreibung des Outsourcing-Vorhabens, detaillierte Angaben zu Mengengerüsten, erwarteten Services und Service-Levels (vgl. →Service-Level Agreement) und einen genauen Zeitplan des Projektverlaufes. Ergebnis des RFP-Prozesses ist i.d.R. die Abgabe verbindlicher Angebote, einschließlich detaillierter Preisstrukturen als Basis einer finalen Auswahl des Outsourcing-Providers.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Responsibility Matrix	<p>Detaillierte Übersicht über die in einem Outsourcing-Vertrag zwischen Dienstnehmer und Dienstleister geregelten wechselseitigen Verantwortlichkeiten. Insbesondere sind hier auch die Mitwirkungspflichten des Kunden festgelegt.</p> <p>S: -, K: Vertrag, O: -, M: Vertragskomponente</p>
Retained Organization	<p>Organisationseinheiten und Mitarbeiter, die im Rahmen eines Outsourcing-Projektes beim Dienstnehmer verbleiben und die Schnittstelle zum Dienstleister bilden. In dieser Organisation sollten sowohl Managementkompetenz als auch (IT-)Fachkompetenz vorhanden sein.</p>

Begriff	Beschreibung
	<p>Zu den Aufgaben dieser Einheit zählen z.B. Definition und Verfolgung der (IT-)Strategie, Anforderungspriorisierung, Schnittstelle zwischen Fachbereich und IT, (IT-)Budgetierung und Freigabe.</p> <p>S: -, K: Lösung, O: -, M: -</p>
Rückabwicklung	<p>Die Rückübertragung der (IT-)Verantwortung in die eigene Organisation (vgl. auch →Insourcing) oder an einen anderen externen Dienstleister bei geplanter oder auch vorzeitiger Beendigung eines Outsourcing-Vertrages. Schon bei Abschluss des Vertrages sollte eine Vereinbarung getroffen werden, die den Dienstleister verpflichtet, Personal, Hardware, Software zurückzuführen oder zu übertragen und dem Kunden angemessene Unterstützungsleistungen im Rahmen seines Insourcing-Projektes zu gewähren. Gleiches gilt natürlich auch bei einem Wechsel des Dienstleisters.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Scope	<p>Inhaltlicher Leistungsumfang des Outsourcing-Vertrages (was wird wann wie von wem geleistet).</p> <p>S: Outsourcing Scope, K: Vertrag, O: -, M: Vertragskomponente</p>
Selective Outsourcing	<p>1. Vergabe von einzelnen - möglichst sachlich zusammenhängenden - (IT-)Aufgaben (z.B. Desktop-Services) im Rahmen von Outsourcing-Vorhaben an einen oder verschiedene externe Dienstleister i.d.R. einschliesslich Übertragung von Unternehmenswerten und Personalübergang (→Asset- und →Personnel Transfer ; vgl. auch im Gegensatz dazu: →Total Outsourcing oder →Multi Sourcing).</p> <p>2. Häufig auch gleichgesetzt mit →Outtasking. Allerdings findet beim Outtasking i.d.R. kein Asset- und Personal-Transfer statt.</p> <p>S: Smart Outsourcing; Smart Sourcing; Best of Breed Outsourcing; →Partielles Outsourcing, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Service Management	<p>Prozess, der die Einhaltung vereinbarter →Service-Level Agreements (SLA) und die zielgerichtete, unmittelbare Einleitung von Maßnahmen bei Abweichung durch den Dienstleister sicherstellt.</p> <p>S: -, K: Service-Management, O: -, M: Prozess</p>
Service Center	<p>Der Begriff ist doppelt belegt:</p> <ul style="list-style-type: none"> ■ Organisatorische Einheit in einem Unternehmen, das eine bestimmte Service-Leistung intern für mehrere Unternehmenseinheiten erbringt. Die interne Konsolidierung/Bündelung von IT-Leistungen in einem Service Center kann die Vorstufe zu einem Outsourcing sein.

Begriff	Beschreibung
	<p>■ Externer Dienstleister, der spezialisierte Service-Leistungen für mehrere Unternehmen bereitstellt (vgl. →Shared Services).</p> <p>S: Shared Service Center, K: Lösung, O: -, M: Shared Service Center</p>
Service-Level Agreement(s)	<p>Schriftliche Vereinbarung zwischen dem Outsourcing-Dienstleister und dem Kunden über die Qualität und Quantität der im Rahmen des Outsourcing-Vertrages zu erbringenden Service-Leistungen anhand eindeutig nachweisbarer und nachvollziehbarer Kriterien.</p> <p>Bestandteile eines SLA sind z.B.:</p> <ul style="list-style-type: none"> ■ Leistungsdefinitionen, ■ Servicezeiten, ■ Reaktionszeiten ■ Support-Zeiten <p>S: -, K: Service-Management, O: -, M: Vertragskomponente</p>
Service-Level Management	<p>Prozess zur Sicherstellung der Erfüllung der Service-Level Agreements (→SLA) durch den Servicegeber und die Kontrolle durch den Servicenehmer. Im Zuge des Service-Level Managements werden die vertraglich vereinbarten SLA periodisch überprüft und mit dem Kunden durchgesprochen. Sollte dabei deutlich werden, dass bestimmte Services nicht mehr den Anforderungen des Kunden entsprechen wird ein entsprechender →Change Request eingeleitet. Bei Untererfüllung der SLA werden zielgerichtete Maßnahmen zur Verbesserung eingeleitet. Basis von Service-Level Management ist Service Monitoring und Service Reporting.</p> <p>S: -, K: Service-Management, O: -, M: Prozess</p>
Service-Level Objective(s)	<p>Zielgrößen, die in den Service-Level Agreements definiert sind. SLO sind die quantitativen und/oder qualitativen Vorgaben, die für alle Service-Aktivitäten, -Funktionen und -Prozesse erreicht werden müssen.</p> <p>S: -, K: Service-Management, O: -, M: -</p>
Share Deal	<p>(IT-)Outsourcing in Form einer Unternehmensbeteiligung. Gegenstand des Kaufvertrages bei einem Share Deal ist die gesellschaftsrechtliche Beteiligung (z.B. Aktien-/ GmbH-Anteile) am Träger des Unternehmens (vgl. auch →Joint Venture). Die Zuordnung aller Aktiva und Passiva verbleibt unverändert bei der Gesellschaft; lediglich die Besitzverhältnisse verändern sich. Im Gegensatz hierzu steht der →Asset-Deal.</p> <p>S: -, K: Vertrag, O: -, M: Vertragskomponente</p>

Begriff	Beschreibung
Shared Services	<p>Beim Shared Service Modell nutzen mehrere Unternehmen oder mehrere Abteilungen eines Unternehmens gleiche Leistungsbereiche, die von einem Shared Service Center bereitgestellt werden. Shared Service Center werden vom Unternehmen selbst oder von spezialisierten Dienstleistern betrieben. Shared Service Modelle eignen sich für Back Office- Funktionen, wie z.B. das Rechnungswesen. Aufgrund der Größe des Centers können Skaleneffekte erzielt werden (vgl. →Service Center).</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>
Single Vendor Outsourcing	<p>Alle auszulagernden (IT-)Aufgaben werden an einen einzigen externen (IT-) Dienstleister übertragen (vgl. auch im Gegensatz dazu →Multi Vendor Outsourcing).</p> <p>S: Single Sourcing, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Sourcing	<p>Prozess der Beschaffung von unternehmensinternen oder -externen Ressourcen.</p> <p>S: -, K: Sourcing, O: Sourcing, M: Prozess</p>
Sourcing Strategy	<p>Die Zusammenfassung von Szenarien, Plänen, Massnahmen und Entscheidungen für die unternehmensinterne (→Insourcing) oder unternehmensexterne (→Outsourcing) Beschaffung von Ressourcen zur Erreichung der Unternehmensziele.</p> <p>S: -, K: Sourcing, O: -, M: Strategie</p>
Statement of Work	<p>Beschreibung der vom Kunden geforderten Dienstleistungen - einschließlich genauer Informationen über die bestehende (IT-)Betriebsumgebung – um sicherzustellen, dass die Leistung bedarfsgerecht und zu dem vereinbarten Preis geliefert wird. Wesentliche Elemente eines SOW beinhalten z.B.:</p> <ul style="list-style-type: none"> ■ Projektinhalt (Scope) ■ Beschreibung der Dienstleistungen ■ Service-Umgebung ■ Service-Levels und Pönalen ■ Rollen und Verantwortungen ■ Ressourcen-Nutzung ■ Preisinformationen <p>S: -, K: Vertrag, O: -, M: Vertragskomponente</p>
Steady State	<p>Mit Beginn des Regelbetriebes vertraglich festgelegter Zielzustand der (IT-)Umgebung des Kunden, ab dem die Outsourcing-Leistung mit den vereinbarten Service-Levels (→Service-Level Agreement (SLA)) erbracht</p>

Begriff	Beschreibung
	<p>werden kann.</p> <p>S: -, K: Lösung, O: -, M: Zustand</p>
Strategic (Out)-Sourcing	<p>Beschreibt Outsourcing als einen wichtigen Bestandteil der Umsetzung mittel- bis langfristiger Unternehmensziele im Rahmen einer umfassenden IT- und Geschäftsprozess-Sourcing-Strategie (z.B. Konzentration auf das Kerngeschäft)</p> <p>S: -, K: Sourcing, O: Sourcing, M: Strategie</p>
Tactical Outsourcing	<p>Der Begriff wird mehrdeutig verwendet:</p> <ol style="list-style-type: none"> 1. Outsourcing-Entscheidung aufgrund kurzfristiger taktischer Überlegungen (z.B. sofortige Kostenreduktion) 2. Outsourcing von Teilaufgaben (vgl. auch →Selective Outsourcing). <p>S: -, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Total (IT-) Outsourcing	<p>Zwei Formen sind denkbar:</p> <ol style="list-style-type: none"> 1. Vollständige Übertragung der (IT-)Aufgaben eines Unternehmens an einen externen Dienstleister. Mit dem Total Outsourcing ist immer der Transfer von Mitarbeitern und Assets verbunden (vgl. →Personnel Transfer und →Asset Transfer). Total Outsourcing ist eine heute eher selten genutzte Option (vgl. im Gegensatz dazu: →Selective Outsourcing). Die Vertragslaufzeit liegt in der Regel zwischen 5 und 10 Jahren und ist damit wesentlich länger als z.B. beim →Hosting. 2. Verkauf einer ausgegliederten (IT-)Gesellschaft („(IT-)GmbH“) an einen externen Dienstleister (vgl. →Share Deal und →Asset Deal). <p>S: Fullscope Outsourcing; Full Outsourcing, K: Outsourcing, O: Outsourcing, M: Strategie</p>
Transformational Outsourcing	<p>Outsourcing einer bestehenden veralteten oder inhomogenen IT-Infrastruktur mit dem Ziel, diese in eine „state of the art“ Architektur“ zu überführen.</p> <p>S: -, K: Outsourcing, O: Outsourcing, M: Dienstleistung</p>
Transformation	<p>Veränderung einer bestehenden Geschäftsprozess-Struktur und/oder IT-Infrastruktur und deren Ressourcen mit dem Ziel, signifikante quantitative und qualitative Verbesserungen zu erreichen. Oft ist diese organisatorische und technische Transformation mit der Übernahme von Geschäftsprozessen (→Business Transformation Outsourcing BTO) und/oder der IT-Verantwortung (→Infrastructure Outsourcing - ITO) durch einen externen Dienstleister verbunden.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>

Begriff	Beschreibung
Transition	<p>Phase innerhalb eines Outsourcing-Projektes, in der der Outsourcing-Dienstleister z.B. Mitarbeiter, Daten, Hardware, Software, Leistungen von Drittanbietern, IT- und Geschäftsprozesse des Kunden rechtlich, inhaltlich und physisch in seine Verantwortung übernimmt. Beispielsweise wird das IT-Equipment des Kunden in das Rechenzentrum des Dienstleisters umgezogen.</p> <p>S: -, K: Outsourcing-Prozess, O: -, M: Prozess</p>
Transitional Outsourcing	<p>Auslagerung einer veralteten IT-Infrastruktur an einen externen Dienstleister, um unternehmenseigene Ressourcen auf die Implementierung neuer Systeme und Anwendungen zu konzentrieren.</p> <p>S: -, K: Outsourcing, O: Outsourcing, M: Dienstleistung</p>
Utility Services	<p>Bedarfsgerechte Bereitstellung von IT-Dienstleistungen durch einen externen Service-Provider und deren verbrauchsabhängige Rechnungsstellung; d.h. der Kunde bezahlt nur die tatsächlich abgenommenen Leistungseinheiten („IT aus der Steckdose“). Diese Art der Kapazitätsbereitstellung reduziert und flexibilisiert die operationalen IT-Kosten und erhöht die Anpassungsfähigkeit der IT an die Geschäftsentwicklung (vgl. → On Demand Outsourcing).</p> <p>S: IT Utility Services; Utility Outsourcing; On demand Computing; Metered Services, K: Pricing, O: -, M: Preis-Modell</p>
Wertschöpfungsstruktur	<p>Durch die funktionsübergreifende Verkettungen von Aktivitäten werden wertschöpfende Leistungen erzeugt. Ein entsprechendes Bündel von wertschöpfenden Leistungen lässt für den Empfänger dieser Leistungen (oftmals der Kunde) wettbewerbsdifferenzierende Mehrwerte entstehen.</p>

9 Sachwortverzeichnis

- § 613 a BGB 51
- Abgabenordnung 8, 22, 26
- Abschlussprüfer 23, 25, 30, 31, 36, 39
- Abschlussprüfung 30, 31
- AktG 8, 18, 23, 40, 41, 65
- American Institute of Certified Public Accountants 8, 31
- Änderung
 - antizipierbar 44
- Änderung des Leistungsumfang 44
- Änderungsverfahren 46
- Angemessenheitsentscheidungen der EU-Kommission 57
- Anlagevermögen 51
- Arbeitnehmerdaten 58
- Arbeitskreis Outsourcing 2, 8
- Archivierungsservice 56
- Audit 9, 36, 60, **62**, 63, 64
- Aufsichtsbehörde 52, 53
- Auftragsdatenverarbeiter 25
- Auftragsdatenverarbeitung 12, 25, 43, 48, 56, 68
- Ausfallrisiko 27
- Auslagerung 14, 15, 19, 20, 21, 23, 24, 28, 31, 39, 40, 64, 68
- Auslagerung der IT 40
- Auslagerung Prozesse
 - geschäftskritischer Prozess 27
- Ausspähen von Daten 40
- Automatisierung 14
- BAKred 8, 28, *Siehe* BAFin
- Bankaufsichtsrecht 39
- Bankenerlaubnis 39
- Bankensektor 39
- Basel II 12, 15, 22, 26, 27, 60
- Berichts- und Informationspflicht 48
- Best Practice 34, 52, 53
- Best-Practice-Ansatz 36
- Betrieb von Rechenzentren 13
- Betriebs- und Sicherheitskonzept 63
- Betriebsprüfung 27
- Betriebsrat 58
- Bewerberdaten 58
- BGH 8, 40
- BGHZ 8, 34
- BITKOM 2, 8, 11, 39, 40, 56, 91
- BPO *Siehe* Business Process Outsourcing
- Briefgeheimnis 40
- BS 7799 32, 60, 61, 62, 63
- BSI *Siehe* Bundesamt für Sicherheit in der Informationstechnik
- BSI-Grundschutz 22, **32**, 62
- Buchführung 8, 22, 24, 26, 28, 29, 30
- Buchführungsgrundsätze bei IT-Einsatz 29
- Buchführungspflicht 24
- Buchhaltung 24, 53
- Bundesamt für Sicherheit in der Informationstechnik 8, 13, 19, 22, 32, 47, 61, 62
- Bundesanstalt für die Finanzdienstleistungsaufsicht 8, 13, 15, 19, 27, 28, 39
- Bundesdatenschutzgesetz 8, 15, 18, 22, 25, 39, 43, 48, 56, 57, 58, 68
- Bundesgesetz 18

Business Continuity 46
 Business Process Outsourcing 8, 64
 Business Recovery 46
 Certification bodies 63
 Change-Request 44
 Change-Request-Prozess 45
 Change-Request-Verfahren 44
 CoBIT 8, 20, 22, 35, **36**, 54, 66, 67, 68
 Committee of Sponsoring Organizations of
 the Treadway Commission 8
 Commodity 14
 Compliance 1, 2, 3, 10, 12, 13, 22, 32, 36, 59
 Control Effectiveness 66
 Control Objectives 8, 36
 Control Objectives for Information and
 Related Technology 36
 Corporate Governance 3
 Corporate Governance Codex 19, 65
 COSO 8, 22, **35**, 36
 D & O-Versicherung 41
 Data Protection Code of Conduct 58
 Daten
 personenbezogene 25
 Datenarchivierung 27
 Datenerhebung
 Zulässigkeit 25
 Datenhistorisierung 27
 Datenschutz 12, 39, 44, 50, 56, 57, 58, 59, 60,
 61
 Datenschutzbeauftragter 39
 Datenschutzbehörde 58
 Datenschutzgesetz 58
 Datenschutzniveau 25
 Angemessenheitsentscheidung 25
 Datenschutzrecht 39
 Datensicherheit 44, 50, 66
 Datensicherungs-Prozess 27
 Datenübertragung innerhalb der EU 57
 Datenwiederherstellungs-Prozess 27
 De-facto-Standard 47
 Design Effectiveness 66
 Deutsches Institut für Normung e.V. 8
 Dienstleistungs-Anbieter 35, 52
 Dienstleistungs-Unternehmen 17, 18, 30, 31,
 53
 DIN 8, 19, 28, 34
 Disaster Recovery 46
 Dissens
 versteckter 42, 43
 Eigenkapitalvereinbarung 27
 Einwilligung der Betroffenen 58
 EN ISO 9000 ff. 34
 Enterprise Resource Planning 8
 Entlastungsstrategie 73
 Erweiterungsstrategie 73
 Eskalation 42
 Eskalationsprozess 45
 EU-Datenschutzrichtlinie 95/46/EG 25
 EU-Kommission 57
 Europäische Kommission 57, 68
 European co-operation for Accreditation 63
 EU-Standardvertragsklausel **57**, 68
 Exit Management **51**
 Exit-Plan 51
 Fachausschuss für Informationstechnologie
 29
 FAIT *Siehe* Fachausschuss für
 informationstechnologie

FAIT 1 29
 Finanzbuchhaltung 27
 Firewall 43, 47
 Fortführung der kritischen
 Unternehmensprozesse 46
 Funktionsübertragung 25
 Gap-Analyse 63
 GDPdU 8, 22, 26
 Gehaltsabrechnung 56
 Geräte- und Produktsicherheitsgesetz 39
 Geschäftsführung
 Verantwortung 12, 17
 Geschäftsprozess 17, 18, 59
 • IT-gestützter 29
 Geschäftsumfeld
 dynamisches 44
 Gesetz **18, 23**
 Globalisierung 12
 GmbHG 8, 22, 24, 40
 GoBS 8, 22, 28, 29, 66
 Governance 9, 19, 20, 42, 45, 65
 Grenznutzen 46
 Grundsätze ordnungsgemäßer Buchführung
 24, 28
 Grundsätze ordnungsgemäßer DV-
 gestützter Buchführungssysteme 28
 Grundsätze zum Datenzugriff und zur
 Prüfbarkeit digitaler Unterlagen 8, 26
 Haftung 2, 21, 23, 24, 39, 40, 41
 Haftungsregelung 40
 Haftungsrisiko 38, 39
 Haftungsverpflichtung 17
 Haftungsverpflichtung für ausgelagerte
 Prozesse 17
 Handelsgesetzbuch 8, 24
 Handelsrecht 24
 Hardwarewartungsvertrag 51
 HGB 8, 22, 23, 24, 28, 39
 HR Management 64
 IDW PS 330 22, 30, 31
 IDW PS 331 22, **31**, 55
 IDW RS FAIT 1 22, 29
 IEC 8, 34
 Information Systems Audit Control
 Foundation 36
 Information-Lifecycle-Management 40
 Informations-Risiko-Management 61
 Informations-Sicherheit 13, 32, 61
 Informations-Sicherheits-Management 61
 Informations-Sicherheits-Management-
 System 34, 61
 Informationstechnologie 8, 12, 29, 30, 60
 Infrastruktur 13, 36, 60, 67
 Insourcing 51
 Institut der Wirtschaftsprüfer 28
 International Organization for
 Standardization 9
 Interne Revision 65
 Internes Überwachungssystem 65
 ISO 9, 13, 19, 22, 28, 32, 34, 35, 54, 60, 61, 62
 ISO 14000 62
 ISO 17799 22, **32**, 35, 60, 61, 62
 ISO 27001 32
 ISO 9000 62
 ISO 9001 35
 ISO/IEC 27001 34
 ISO/IEC 9126 34
 IT
 Beitrag zum Unternehmenserfolg 12

Kostenfaktor 14
 IT Governance Institute 9, 20
 IT Infrastructure Library 9, 42
 IT-Anwendung 29
 IT-Betrieb 14, 15
 IT-Governance 20, 21
 IT-Grundschutz 32
 IT-Grundschutzhandbuch 32, 61
 ITIL 9, 20, 22, 35, **36**, 41, 42, 53, 54, 62
 IT-Infrastruktur 29
 IT-Kontrollen **29**
 IT-Kontrollsystem 29
 IT-Kontroll-System 36, 67, 68
 IT-Organisation 14, 15, 36
 IT-Organisation 13
 IT-Organisationsmodell 13
 IT-Outsourcing 2, 3, 9, 10, 11, 12, 13, 15, 17, 20,
 22, 30, 31, 32, 35, 36, 39, 91
 IT-Outsourcing-Projekt 3, 25
 IT-Risiko-Management 27
 IT-Service-Management 20, 36
 IT-Sicherheit 21, 32, 40, 59, 60, 61
 IT-Sicherheits-Management 32
 IT-Sicherheitsmaßnahme 32
 IT-Sicherheitsniveau 59
 Jahresabschlussprüfer 53
 Jahresabschlussprüfung 23, 53, 66
 Kennzeichnungssystem für Backups 47
 Kernkompetenz 13, 14, 15, 91
 Key Performance Indicator 9, 42
 Komplexität 15, 21, 23, 54, 56
 kontinuierlicher Verbesserungsprozess 9, 15,
 60
 KonTraG 9, 15, 22, 23, 60, 66
 Kontroll- und Steuerungsmechanismus 42
 Kontroll-Management 46
 Kontrollsystem
 internes **29**
 Kontroll-System 26, 30, 31, 32, 34, 35, 36, 48,
 59, 66, 67, 68
 Kontrollverlust 15
 Kosten 10, 13, 14, 15, 43, 44, 45, 46, 47, 48, 49,
 52, 53, 55
 Kreditinstitut 27
 Kreditvergabe 27
 Kreditwesengesetz 9
 Kündigung 46, 49, 50, 51
 Kündigungsrecht 42, 45
 Landesgesetz 18
 Leistungsbeschreibung **42**, 43, 44
 Leistungserbringung 10, 43, 44, 45, 49, 50, 51
 Leistungsparameter 49
 Messung 42
 Leistungsqualität 48
 Leistungsumfang 44, 45, 50
 Leistungsvereinbarung 48
 Leistungsvolumen 44
 Messinstrument 49
 Mitarbeiterschulung 47
 Mittelstand 13, 15
 mittelständisches Unternehmen 13, 15
 Mitwirkungspflicht 42
 Monitoring 63
 Nachfolge-Dienstleister 51
 Nearshoring 10
 Nichteinhaltung rechtlicher
 Rahmenbedingungen 39
 Notfall 46, 47

Notfallkonzept 46, 47, 49
 Notfallplanung 27, 46, 47
 Notfallszenarium 49
 Öffentliche Verwaltung 32
 Office of Government Commerce 9, 20
 Offshore 2, 91
 Offshoring 10
 One-to-One Solution 45
 Ordnungsmäßigkeit 12, 15, 29, 30, 32, 53
 Ordnungsmäßigkeits-Kriterien 28
 Ordnungswidrigkeitenrecht 38
 Organisation der Sicherheit 60
 Outsourcing
 Buchhaltung 24
 Finanzbuchhaltung 26
 steuerlicher Aspekt 21
 Verantwortung 17, 18
 versicherungsrechtlicher Aspekt 21
 Outsourcing des Risikos 15
 Outsourcing-Anbieter 23, 27, 31, 32, 35, 36, 56
 Outsourcing-Beziehung 15, 18
 Outsourcing-Deal 36
 Outsourcing-Dienstleister 26, 32
 Outsourcing-Entscheidung 12, 13
 Outsourcing-Projekt 15, 17, 28, 38, 39
 Outsourcing-Service 3, 10
 Outsourcing-Vertrag 3, 11, 44, 50
 Änderungen der rechtlichen
 Rahmenbedingungen 11
 Laufzeit 11
 Template 41
 vorgefertigte Teile 41
 Password-Policy 63
 Penetrationstest 62
 Personalabrechnung 64, 66
 personenbezogene Daten 25, 56, 58
 Post- oder Fernmeldegeheimnis 40
 Preis der Dienstleistung 46
 Preisgestaltung 11
 Preismodell 44
 Primärrecht 18
 Prozessberatung 14
 Prozessgestaltung 14, 54
 Prozesskenntnis 13
 Prozesskompetenz 14
 prozessorientierter Ansatz 35
 Prüfbescheinigung 10, 52, 55
 Prüfrou tine 10, 52
 Prüfungs- und Kontrollrechte 48, 49, 50
 Prüfungs-, Zugangs- und Kontrollrecht 48
 Prüfungs-Standard 54, 55
 Qualität 15
 Qualitäts-Management 34, 35, 62
 Qualitäts-Management-System 35
 Rating 27
 Rechnungslegungs-Dienstleistung 31
 Rechnungslegungs-System 28
 Rechnungslegung-System 30
 rechtliche Rahmenbedingungen
 Änderung 44
 Rechtliche Rahmenbedingungen 43
 Referenzmodell 3, 17, 20, 35, 36, 53, 59, 66, 67
 Regressanspruch 49
 Reifegrad 10, 12, 13
 Restrisiko 46
 Re-Transition 50
 Re-Transition-Projekt 50, 51
 Richtlinie 3, 57, 58, 63

Richtlinien des europäischen Datenschutzes 57

Risiko 9, 12, 15, 19, 23, 26, 27, 28, 30, 32, 40, 41, 44, 45, 46, 48, 59, 61, 65, 67

Risiko im Unternehmen

- Bewertung 13

Risiko Mapping 67

Risikoabschätzung 46

Risikobewertung 44

Risikokontrolle 15

Risiko-Management 9, 15, 19, 23, 26, 27, 28, 32, 40, 41, 48, 59, 61, 65

Risiko-Management-System 23

Risikominimierung 14, 46

Risikovermeidung 46

Risikovorkehrung 27

Safe Harbor 57

Safe-Harbor-Abkommen 68

Sarbanes-Oxley-Act 9, 22, 26, 64

SAS 70 15, 22, 31, 34, 35, 54, 55, 64, 65, 66

SAS 70 Typ I Bericht 31, 34, 66

SAS 70 Typ II Bericht 31, 34

Schadenersatz 42

Schadenersatzanspruch 39

Schutz natürlicher Personen 25

Second-Generation Outsourcing 51

Section 404 26, 64

Securities Act 26

Security Policy 60

Sekundärrecht 18

Service-Level 42, 48, 49, 50, 59

Service-Level-Agreement 9, 36, 42

Service-Level-Vereinbarung 48

Service-Provider 53

Shared Service 45

Sicherheit 60

Sicherheitskonzept 61

Sicherheitsmangel 47

Sicherheitspolitik 60

Sicherheitsprozess 13

Sicherheitsrichtlinie 47

Sicherheitsstandard 17, 32, 60

Sicherheitsziel 61

Skaleneffekt 11

SLA *Siehe* Service-Level-Agreement

Software 44

Softwarepflegevertrag 51

Softwarequalität 34

Sorgfalt 2, 34, 40, 41, 46

Sourcing 14

Sourcing-Entscheidung 12

SOX 9, 13, 15, 26, 31, 36, 55, 64, 65, 66

SOX-Anforderungen 26, 31, 55

Spezifikation 42

SSL-Verschlüsselung 63

Standard 3, 19, 28, 29, 30, 31, 32, 34, 35, 43, 53, 54, 55, 60, 61, 67, 68

Standardisierung 11, 14, 35, 53, 55

Standardisierungsgrad 54

Statement on Auditing Standards 9, *Siehe* SAS

Steuerungssystem

- internes 29

Strafrecht 38, 39

strafrechtlichen Verantwortlichkeit 38

Supply Chain 12

System

- kritisches 27

Telekommunikations-
kündigungsvorordnung 19

Template 41

Terminologie 2, 10, 91

TÜV Industry Service GmbH 63

Übermittlung
personenbezogene Daten 25

Überwachungspflicht 41

Überwachungssystem 23, 29

Unternehmens-IT 13, 66

Unternehmensstrategie 36

Unterstützungsleistung 51

Verantwortung der Geschäftsleitung 40, 59

Verarbeitung personenbezogener Daten 25

Verbindliche Unternehmensregelung **58**

Vereinheitlichung 55

Verlagerung 10, 15

Verletzung datenschutzrechtlicher
Bestimmungen 39

Vernetzung zwischen Kunden und
Lieferanten 12

Versicherungsvertrag 21

Vertrag 18, 43, 47, 48, 49, 51

Vertragsbeendigung 50

Vertragsgestaltung 21, 41, 46

Vertragslaufzeit 44, 50

Verwaltungsakt 19

Virenschanner 43, 47

Volumenänderung 44

Vorsorgemaßnahme 47

Wertbeitrag der IT-Organisation 15

Wertschöpfung 13, 14

Wertschöpfungsbeitrag 14

Wertschöpfungsgrad 14

Wertschöpfungsrelevanz 14

Wettbewerbsposition 15

Wiederanlaufplan 46

Wirtschaftlichkeitsbetrachtung 11

Wirtschaftlichkeitsrechnung 11

Wirtschaftsprüfer 8, 23, 26, 28, 29, 30, 31, 32,
36, 53, 65, 66

Wirtschaftsprüfung 13, 22, 28, 53, 67

Wirtschaftsprüfungsstandard 31

Wirtschaftsprüfungs-Standard 29

Zentralisierung von Dienstleistungen 11

Zertifikat 3, 60, 62, 64

Zertifizierung 22, 30, 31, 32, 35, 36, 52, 60, 61,
62, 63, 64

Zertifizierungs-Standard 54

Zugangsberechtigungs-System 27

Zugangskontrolle 60

Zugriffsschutz 66

10 BITKOM-Arbeitskreis Outsourcing

Tabelle 9: Kurzprofil des Arbeitskreises Outsourcing

■ Gründung, Aufgaben und Ziele

Im Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) haben Mitgliedsunternehmen am 27. April 2004 den Arbeitskreis „Outsourcing“ (kurz: AK OSC) gegründet, der sich an alle Interessenten im Verband wendet, die Dienstleistungen im Bereich des IT-Outsourcing anbieten. Im AK OSC engagieren sich die führenden Anbieter auf dem deutschen Markt sowie zahlreiche kleine und mittelständische Unternehmen. Im AK OSC wird Outsourcing als allgemeiner Oberbegriff für die vollverantwortliche Übertragung betrieblicher Funktionen außerhalb der Kernkompetenz von Unternehmen an externe Dienstleister zur Verminderung der Fertigungstiefe verstanden.

Der AK OSC gehört zum BITKOM-Kompetenzbereich IT-Services. Der Kompetenzbereich will dazu beitragen, dass IT-Dienstleistungen als eigenständiges Marktsegment wahrgenommen werden. Damit soll er die Positionierung der auf IT-Services spezialisierten Anbieter bei den Kunden verbessern. Ziel des Outsourcing-Arbeitskreises ist die Schaffung von Rahmenbedingungen, unter denen sich der Markt für ITO entfalten kann.

■ Aktivitäten und Themen

Konzipierung und Umsetzung gemeinsamer Projekte vorrangig in Öffentlichkeitsarbeit und Marketing wie „BITKOM-Positionierung zum Thema ITO“, „Leitfaden erfolgreiches Outsourcing“, „Anwenderforum Outsourcing“, „ITO Terminologie“, „Offshore-Leitfaden“, „IT-Outsourcing im Öffentlichen Dienst“ oder „Offshore-Report 2005“, Best-Practice-Darstellungen, Benchmarking, Erfolgssteuerung in ITO-Beziehungen.

Vermittlung von neuestem Management-, Markt- und Technologiewissen, insbesondere durch den Erfahrungsaustausch zwischen BITKOM-Mitgliedern.

Durchführung von Foren und Arbeitskreis-Meetings zu strategisch relevanten und aktuellen Themen. Networking mit Anwendern und Organisationen. Mitgestaltung wirtschaftspolitischer, rechtlicher und soziokultureller Rahmenbedingungen für ITO.

■ Ansprechpartner

Vorsitzender des AK OSC ist Christian Oecking (Siemens Business Services GmbH & Co. OHG).
Stellvertreter: Dr. Stephan Scholtissek (Accenture).

Weitere Mitglieder im Vorstand sind Thomas Genter (IBM Deutschland GmbH),
Dr. Jens Gerber (e-nable.biz GmbH) und Klaus Nötzold (T-Systems International GmbH).

Der AK OSC wird beim BITKOM betreut von Dr. Mathias Weber

(Telefon: 030/27576-121, Fax: 030/27576-400, E-Mail: m.weber@bitkom.org).

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.000 Unternehmen, davon 800 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin

Tel.: 030/27 576-0
Fax: 030/27 576-400

www.bitkom.org
bitkom@bitkom.org
