



Xpert.press

Frank A. Koch

IT-Projektrecht

 Springer



Xpert.press

Frank A. Koch

IT-Projektrecht

 Springer

Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals
in den Bereichen Softwareentwicklung,
Internettechnologie und IT-Management aktuell
und kompetent relevantes Fachwissen über
Technologien und Produkte zur Entwicklung
und Anwendung moderner Informationstechnologien.

Frank A. Koch

IT-Projektrecht

Vertragliche Gestaltung und Steuerung
von IT-Projekten, Best Practices,
Haftung der Geschäftsleitung

Dr. Frank A. Koch
Maximilianstr. 54
80538 München
koch@anwaltskanzlei-koch.de

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.ddb.de> abrufbar.

ISSN 1439-5428
ISBN 978-3-540-73223-5 Springer Berlin Heidelberg New York

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

© Springer-Verlag Berlin Heidelberg 2007

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Text und Abbildungen wurden mit größter Sorgfalt erarbeitet. Verlag und Autor können jedoch für eventuell verbliebene fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Satz und Herstellung: LE-TeX, Jelonek, Schmidt & Vöckler GbR, Leipzig
Umschlaggestaltung: KünkelLopka Werbeagentur, Heidelberg

Gedruckt auf säurefreiem Papier 33/3180 YL - 5 4 3 2 1 0

Vorwort

Verträge für die unterschiedlichsten IT-Projekte haben eines gemeinsam: Sie müssen die Projekte steuerbar machen und mit ihnen oft verbundene Risiken rechtzeitig ausschalten oder zumindest reduzieren. Solche Risiken sind mannigfaltig. Dies wird durch den Umstand belegt, dass weniger als ein Drittel aller IT-Projekte den versprochenen Leistungsumfang zum geplanten Zeitpunkt, im geplanten Budget und mit der spezifizierten Qualität erreicht. Dies führt betriebswirtschaftlich zu nicht unerheblichen Schäden, die sich durch geeignete Gestaltung und Durchführungskontrolle von IT-Projektverträgen weitgehend vermeiden lassen. Die wichtigsten Best Practices hierzu werden in der vorliegenden Darstellung zusammengefasst.

Die mit IT-Projekten verbundenen Risiken sind umso gravierender, je tiefer die IT in die Steuerung der betrieblichen Abläufe eingreift. Sie können sogar den Bestand des anwendenden Unternehmens bedrohen, wenn dessen Wettbewerbsfähigkeit deutlich beeinträchtigt wird, so etwa durch Verlust geplanter Rationalisierungs- oder Marktvorteile. Der gesamte produktive Betrieb kann gefährdet sein, wenn zum Beispiel die Einführung von sog. „Enterprise Resource Planning“-Software scheitert, die alle wesentlichen Geschäftsprozesse hätte steuern sollen, und wenn zugleich die alte Anwendung anbieterseits nicht mehr oder nur eingeschränkt unterstützt wird. Ein weiteres Risiko ergibt sich aus Defiziten in der unzureichenden technischen Sicherung der jeweiligen Anwendungen, die einerseits die Nutzbarkeit des IT-Systems in der gesamten vorgesehenen Nutzungsdauer sicherstellen, und andererseits, oft genauso wichtig, Angriffe von außen auf die betriebliche IT abwehren soll. Auch hier muss eine Gestaltung von Verträgen mit Dienstleistern den bestehenden Risiken angemessen Rechnung tragen. Das Herstellen und laufende Unterstützen der IT-Sicherheit ist selbst als – oft für den Unternehmensbestand wesentliches – Projekt zu konzipieren.

Betrachtet man Fälle gescheiterter IT-Projekte näher, so zeigt sich, dass meist keine ausreichende Vorsorge für zeitnahe Projektsteuerung und Absicherung der Anwendungen in den zugehörigen Projektverträgen getroffen wurde, obwohl sie möglich gewesen wäre. Insbesondere werden oft nur Leistungsziele vorgegeben (und auch diese nicht selten nur ungenau), nicht aber die Wege zu diesen Zielen mit kontrollfähigen Zwischenschritten im Projektablauf vertraglich definiert. Die vorliegende Darstellung soll aufzeigen, welche Regelungspunkte ein IT-Projektvertrag aufweisen muss, der zu einer erfolgreichen Projektsteuerung beitragen kann. Die Darstellung ist **nach den typischen Stufen von IT-Projekten aufgliedert** und diskutiert auf

jeder Stufe Fallstricke und mögliche Vorkehrungen gegen solche Risiken. Berücksichtigt sind die Best-Practice-Vorgaben von ITIL und die hieraus entwickelten typisierten Regelungsvorschläge in der Norm ISO 20000. Diese in der Praxis entwickelten Vorgaben für Regelungspunkte nicht einzubeziehen, kann einen gravierenden Fehler bei der Vertragsgestaltung (und Rechtsberatung) darstellen.

Die Durchführung von IT-Projekten stellt selbst geradezu ein Musterbeispiel für ein Risiko dar, das jede Geschäftsleitung aus ihrer Rechtspflicht früherkennen und abwenden oder zumindest begrenzen muss. Mit zunehmender Bedeutung der IT für die Steuerung praktisch aller Geschäftsprozesse im Unternehmen steigt das Risiko, dass ein Scheitern des jeweiligen Projekts den Bestand des gesamten Unternehmens gefährden kann (etwa, weil eine notwendige Migration auf andere Systemplattformen oder eine benötigte Einführung oder Änderung von unternehmenssteuernder Software scheitert). Vorsorge gegen diese Risiken kann am ehesten (und teilweise überhaupt nur) über einen entsprechend ausverhandelten Projektvertrag getroffen werden. Diese vertragliche Projektabsicherung herzustellen gehört zu den wesentlichen Aufgaben der Geschäftsleitung IT-anwendender Unternehmen. Für die einzelnen Projektstufen wird deshalb im Text und in Checklisten aufgezeigt, welche Kontrollen IT-Projektleiter und Geschäftsleitung (auch präventiv) durchzuführen haben.

Die Mitglieder der Geschäftsleitung haben ein eigenes Interesse am Gelingen des IT-Projekts. Wäre nämlich das Scheitern oder die erhebliche Verzögerung eines Projekts u. a. durch bessere Vertragsgestaltung und straffe Kontrolle des Projektfortschritts (bzw. eine schadensträchtige Kompromittierung der IT-Sicherheit durch rechtzeitige Kontroll- und Schutzmaßnahmen) und weitere geeignete Maßnahmen im Projektmanagement vermeidbar gewesen, kann das Unterlassen dieser Maßnahmen die persönliche Haftung jedes der Mitglieder der Geschäftsleitung begründen, wenn und soweit das erforderliche Überwachungssystem zur Risikofrüherkennung nicht oder nicht ausreichend eingerichtet und angewendet wurde. Die Mitglieder der Geschäftsleitung haften insoweit dem Unternehmen und damit den Kapitaleignern auf den Ersatz von Schäden, die durch solche Versäumnisse verursacht wurden, müssen also im eigenen Interesse jedenfalls die typischen und damit bekannten und vorhersehbaren Fehler bei der Konzipierung und Durchführung von IT-Projekten vermeiden. Die Darstellung enthält in dieser Hinsicht gewissermaßen ein **Pflichtenprogramm für Projektleiter und Mitglieder der Geschäftsleitung zum richtigen Management von IT-Projekten**. Werden die auf der Grundlage dieses Pflichtenprogramms getroffenen Maßnahmen außerdem zureichend dokumentiert, kann dies zugleich eine Entlastung von möglicher persönlicher Haftung wesentlich erleichtern.

Frank A. Koch
Frühjahr 2007

Inhalt

Vertragsgestaltung für IT-Projekte – zentrale Regelungspunkte im Überblick	1
A Steuerung von IT-Projekten durch Vertrag.....	3
B Stufen der Durchführung von IT-Projekten.....	7
1. Anforderungsphase – Feststellen der IT-Anforderungen durch den Kunden	7
a) Projektvorschlag.....	8
b) Analysephase	8
(1) Ist-Analyse.....	9
(2) Reorganisation, Anforderungs- bzw. Systemspezifikation, Sollkonzept.....	10
c) Entscheidung über das IT-Projekt.....	14
(1) Projekttyp	15
(2) Projektstufen.....	16
d) Leistungsbeschreibung.....	17
e) Lastenheft und Pflichtenheft als Formen der Leistungsbeschreibung.....	19
(1) Erstellen der fachlichen Anforderungen (Lastenheft)	19
(2) Erstellung des Lasten-/Pflichtenheftes durch den Anbieter	26
(3) Erstellen des IT-bezogenen Pflichtenhefts und (technischen) Feinkonzepts.....	28
2. Auftragsvergabe, Vertragsschluss, Aufwendungen vor Vertragsschluss	34
3. Dokumentation der Anbieterleistung.....	38
4. Phasen der Software-Erstellung	40
a) Standardlösungen, Parametrisierung, individuelle Anpassungen, Neuerstellung.....	40
b) Portierung.....	41
c) Zusatzfunktionalität	42
d) Prototypen	42
e) Datenmigration	43

f) Projektkosten	44
g) Versteckter Aufwand des Auftraggebers.....	45
h) Vergütung, Festpreis	45
i) Zeitplan für Projektaktivitäten	46
j) Zutritt zu Systemen des Auftraggebers	48
k) Installation.....	48
l) Schulungen	49
5. Projektorganisation und -management	49
6. Change Management	54
7. Mitwirkung des Auftraggebers	58
8. Abnahmeregelungen	62
a) Grundsätze	62
b) Abnahmeregelungen bei Anwendbarkeit von Kaufrecht.....	67
9. Herausgabe der Quellformate (Sourcen) erstellter Programme.....	71
10. Zulässige Nutzung „gebrauchter“ Software?	73
11. Service Level Agreements – Vereinbarungen abgestufter Anbieterleistungen	78
12. Software-Pflege in IT-Projekten.....	82
a) Sicherung der fortlaufenden Nutzung von Software.....	82
b) Service Level Agreements für Software-Pflege und andere Anbieterleistungen	83
c) Pflicht zur Software-Pflege während eines fünfjährigen „Life Cycle“?.....	84
d) Instandsetzung und Instandhaltung.....	86
e) Updates, Versionen, Upgrades	89
f) Fehlerbeseitigungen	90
g) Auf Software-Pflege anwendbares Recht, Mängelhaftung	93
h) Laufzeit von Software-Pflegeverträgen.....	94
13. Regelungen zur Projektbeendigung	95
a) Parallelbetrieb von alter und neuer Anwendung, Beendigungsunterstützung	95
b) Pflichten bei vertragsgemäßigem Projektabschluss.....	95
c) Pflichten bei Projektabbruch	95
14. Qualitätssicherung der Anbieterleistung	96
a) Qualitätsmanagement – zentrale Begriffe und Anbieterpflichten....	100
b) Einrichten und Aufrechterhalten eines Qualitätsmanagementsystems als Vertragspflicht des Anbieters.....	103
c) Auditierung von Qualitätsmanagementsystemen	104
d) Zusammenhang der Normen EN/ISO 9000:2005, 9001:2000 und 9004:2000	106
e) Konfigurationsmanagement	108
f) Dokumentation	108

g) Produktrealisierung.....	109
h) Entwicklung.....	110
i) Lenkung fehlerhafter Produkte.....	112
j) Produktnormen.....	113
k) Informationssicherheit nach ISO 17799.....	116
l) Qualitätsmanagement für Dienstleistungen	116
15. Öffentliche IT-Projekte zur Beschaffung nach den EVB-IT und den BVB.....	117
a) Grundlagen.....	117
b) Besondere Vertragsbedingungen (BVB) und Ergänzende Vertragsbedingungen (EVB-IT)	119
16. Kostensenkungen durch Vertragsanpassungen.....	121
17. Risiken und Sanierung von IT-Projekten.....	128
a) Risiken	128
b) Projektsanierung.....	130
C Rechte des Software-Anwenders bei Insolvenz des Anbieters	135
1. Software-Kauf.....	138
2. Software-Erstellung.....	139
3. Vermietung von Software	139
4. Pflege von Software.....	140
D IT-Sicherheitsmanagement als Projekt.....	141
1. Grundbegriffe des IT-Sicherheitsmanagements.....	142
2. Durchführen des IT-Sicherheitsprozesses als Aufgabe der Leitungsebene (IT-Sicherheitsmanagement)	143
3. Grundlagen des IT-Sicherheitsmanagements.....	145
4. Einrichten und Erhalten des IT-Sicherheitsprozesses	147
5. IT-Sicherheitskonzept	149
6. Aufrechterhalten der IT-Sicherheit.....	150
7. Betriebliche Regelung der IT-Sicherheit.....	151
8. Sicherheitsrichtlinien.....	153
9. IT-Sicherheitsbeauftragter und IT-Sicherheitsmanagement.....	156
10. Dokumentation des IT-Sicherheitsprozesses.....	157
11. Notfallvorsorge-Konzept	158
12. Datensicherungskonzept.....	158
13. Computerviren-Schutzkonzept.....	159
14. Kryptokonzept.....	159
15. IT-Sicherheitssensibilisierung und -schulung	160
16. Managementbewertung der IT-Sicherheit	160
17. Protokollierung am Server.....	161
18. Regelmäßiger Sicherheitscheck des Netzes	161

E	Leistungsstörungen im Projekt	163
1.	Rechte aus Verzug des Auftragnehmers mit der Projektleistung	163
2.	Mängelrechte des Auftraggebers aus Projektverträgen	166
a)	Mängelrechte des Auftraggebers aus Werkvertrag	166
b)	Mängelrechte des Auftraggebers aus Kaufvertrag	170
(aa)	Begriff des „Sachmangels“ im Kaufrecht	170
(bb)	Rechtsmängel	173
(cc)	Mängelrechte des Auftraggebers aus Kauf	173
c)	Haftung aus Garantie	177
d)	Mängelrechte des Auftraggebers aus Mietvertrag	178
(aa)	Anspruch auf Erhaltung der Funktionsfähigkeit der Mietsache – Mängelbeseitigung	178
(bb)	Minderung des Mietzinses	179
(cc)	Schadensersatzanspruch aus Zusicherungsverletzung	180
(dd)	Schadensersatzanspruch des Mieters aus Nichterfüllung	180
(ee)	Fristlose Kündigung	181
3.	Verschulden bei Vertragsschluss (culpa in contrahendo)	183
F	Vertraglicher Rahmen für typische IT-Projekte	187
1.	Einführung von ERP (Enterprise Resource Planning)-Software	187
a)	Absicherung überprüfbarer schrittweiser Projektdurchführung	187
b)	Vermeidung der Übernahme historisch gewachsener Abläufe	187
c)	Vertragsgestaltung	188
d)	Übersicht über die Stufen eines Einführungsprojekts	188
e)	„Customizing“ als Teil der vertraglichen Projektleistung	197
(aa)	Business Reengineering	197
(bb)	Customizing und Anpassungsprogrammierung	197
(cc)	Anwendbares Recht	198
2.	Outsourcing	198
a)	Grundkonzeption	198
b)	Formen des Outsourcing	200
c)	Risiken von Outsourcing-Projekten	201
d)	Auf Outsourcing-Projekte anwendbares Recht	203
e)	Ausschreibung von Outsourcing als IT-Projekt	203
f)	Phasen von Outsourcing-Projekten	204
g)	Abnahme von Outsourcing-Leistungen	206
h)	Zentrale Regelungspunkte in Outsourcing-Verträgen	206
i)	Typische Fehler in Outsourcing-Projekten	209
j)	Backsourcing	209
k)	Offshoring	210
l)	Übergang von Arbeitnehmern	211

3.	Application Service Providing (ASP)	212
a)	ASP als Bündel von Leistungen	213
b)	ASP-typische Formen der Software-Nutzung	214
c)	Anwendbares Vertragsrecht.....	216
(1)	Miete	216
(2)	Auftraggeberrechte aus Dienstvertrag	220
(3)	Auftraggeberrechte aus Werkvertrag	220
d)	Datenspeicherungen als Vertragsleistung	221
e)	Urheberrechtliche Nutzungsrechte	221
f)	Zentrale Regelungspunkte in ASP-Verträgen.....	222
g)	Beteiligung des Betriebsrats.....	225
4.	IT-Projekte im Forschungs- und Entwicklungsbereich	225
G	Rechtliche Verantwortlichkeit der Geschäftsleitung	
	für die Projektdurchführung.....	227
1.	Grundsatz	227
2.	Verantwortlichkeitsverteilung.....	227
3.	Sicherung vor den Unternehmensbestand gefährdenden Risiken.....	231
4.	Risikofrüherkennungssystem	235
5.	Vertretenmüssen	237
6.	Auswirkungen unzureichender IT-Sicherheit auf Kreditvergabe und Versicherungsschutz.....	237
H	ITIL und ISO-Normen als Prüfmaßstab.....	241
1.	ITIL	242
a)	Grundsätze.....	242
b)	Configuration Management.....	247
c)	Availability Management.....	250
d)	Service Level Management	251
e)	Security Management.....	254
f)	Change Management	259
g)	Incident und Problem Management.....	261
(aa)	Incident Management	261
(bb)	Problem Management	263
h)	Weitere Managementaufgaben nach ITIL	266
2.	ISO-Normen als Prüfmaßstab.....	268
a)	ISO 20000.....	268
(aa)	Service Level Agreements (SLA)	270
(bb)	Capacity Management.....	272
(cc)	Incident und Problem Management	273

(dd) Change Management	274
(ee) Information Security Management.....	275
b) ISO 27001 und weitere ISO-Normen	276
I Prüfübersichten	279
1. Prüfübersichten für den Projektleiter (IT-Leiter, „Chief Information Officer“ CIO) des Auftraggebers (Kunden) – Planung und Projektvertrag.....	279
a) Projektvorschlag	279
b) Projektantrag stellen	279
c) Analysephase.....	280
d) Wesentliche Regelungspunkte für IT-Projektverträge	290
e) Hinweise zur Systemauswahl.....	292
f) Hinweise zu System-/Plattformwechsel und Migration	293
g) Prüfung der Vertragserfüllung nach DIN/ISO 9000	293
2. Rechtliches Controlling bei Vertragsschluss und -durchführung durch die Geschäftsleitung.....	294
a) Prüfung vor Entscheidung über das IT-Projekt.....	294
b) Vertragsüberprüfung nach DIN/ISO 9001	295
c) Weitere Prüfpunkte:.....	296
Stichwortverzeichnis	301

Literatur

Schriften des BSI

Bundesamt für Sicherheit in der Informationstechnik (BSI), ITIL und Informationssicherheit – Aspekte der Integration von Incident und Security Management, Version 1.0.1, 2006, Version 1.0.1 Sept. 2006, www.bsi.bund.de, zit. als *BSI, ITIL und Informationssicherheit*.

Bundesamt für Sicherheit in der Informationstechnik (BSI), ITIL und Standards für IT-Prozesse – Prozess-Standards für die Entwicklung der IT-Service-Organisation gemäß ITIL Best Practices, Version 1.0.1, herausgegeben von der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung, KBSt-Brief 1/2006, Okt. 2006, www.bsi.bund.de, zit. als *BSI, ITIL und Standards für IT-Prozesse*.

Weitere Literatur

Balzert, Lehrbuch der Software-Technik. Software-Entwicklung, 2. Aufl. 2001.

Blume, Projektkompass SAP, Arbeitsorientierte Planungshilfen für die erfolgreiche Einführung von SAP-Software, 2. Aufl. 1998.

Bock/Macek/Oberndorfer/Pumsenberger, ITIL – Zertifizierung nach BS 15000/ISO 20000, 2006.

Börner/Buhl/Hellmich/Klett/Moos, Leitdaten IT-Recht. Ein Handbuch für die Unternehmenspraxis, 2004.

Braun, Die Zulässigkeit von Service Level Agreements – am Beispiel der Verfügbarkeitsklausel, 2006.

Brössler/Siedersleben (Hrg.), Softwaretechnik, 1. Aufl. 2000.

Buchta/Eul/Schulte-Croonenberg, Strategisches IT-Management, Wert steigern, Leistung steuern, Kosten senken, 2. Aufl. 2005.

Dietrich/Schirra, IT im Unternehmen, Leistungssteigerung bei sinkenden Budgets – Erfolgsbeispiele aus der Praxis 2004.

Ebert, Systematisches Requirements Management. Anforderungen ermitteln, spezifizieren, analysieren und verfolgen 2005.