

HANSER



Leseprobe

zu

„Praxisbuch IT-Dokumentation“

von Manuela Reiss, Georg Reiss

ISBN (E-Book): 978-3-446-45736-2

Weitere Informationen und Bestellungen unter
<http://www.hanser-fachbuch.de/978-3-446-45736-2>

sowie im Buchhandel

© Carl Hanser Verlag, München

Vorwort

Bei der Erstauflage des Buchs haben wir noch die rhetorische Frage gestellt, warum denn ein Betriebshandbuch noch notwendig sei, wenn doch schon eine Entwicklungsdokumentation aus dem Projekt vorliegt. Diese Frage stellt heute, zehn Jahre und viele Gesetze später, keine IT-Organisation mehr. Es geht also nicht mehr so sehr darum, dass dokumentiert werden muss, sondern eher darum, wie man die vorhandenen Dokumentationsteile miteinander verzahnt und zur Verfügung stellt, damit sie einen Nutzen für die unterschiedlichen Interessentengruppen bieten.

In der Praxis hat sich gezeigt, dass die Organisation der Dokumentation von zentraler Bedeutung für die IT-Organisation ist. Es muss klar sein, für welche Teile der Dokumentation die IT verantwortlich ist und für welche Teile die operativen Fachbereiche; mithin also die Frage, was zur IT-Dokumentation gehört. Mit dazu gehören auch klare Zuständigkeiten innerhalb der IT. Nirgendwo wird das so deutlich wie bei der Anwendungsdokumentation. Bei einer Fachanwendung, z. B. ein Vertriebssystem, sind die Anforderungsbeschreibung und das Fachkonzept vom operativen Fachbereich zu erstellen, das entsprechende Betriebskonzept sowie das Betriebshandbuch von der IT-Seite. Eine klare Zuständigkeits- und Verantwortungsabgrenzung sind hier notwendig, um Redundanzen und ggf. Fehler zu vermeiden. Aufgrund dieser aus der Praxis abgeleiteten Erkenntnis haben wir der Anwendungsdokumentation, bestehend aus Entwicklung und Betrieb, erstmals ein eigenes Kapitel gewidmet.

Ein weiteres neues Schwerpunktthema sind die Bereiche Informationssicherheit und Datenschutz, die durch das IT-Sicherheitsgesetz und die DSGVO in Verbindung mit BDSG-neu nochmals an Bedeutung gewonnen haben. Diese Bereiche gehören zu den Querschnittsaufgaben, die vom IT-Management bis in den IT-Betrieb reichen. Es reicht nicht aus, entsprechende Managementkonzepte zu erstellen, sondern die Umsetzung im Betrieb muss durch konkrete Maßnahmen nachgewiesen werden. Zusammen mit der Notfalldokumentation, ebenfalls ein Querschnittsthema, sind die beiden Bereiche in einem gesonderten Kapitel dargestellt.

Wie der Buchtitel „Praxisbuch IT-Dokumentation“ schon andeutet, liegt die Ausrichtung des Buchs auf dem IT-Betrieb. Jedoch machen die beiden neuen Schwerpunktthemen auch deutlich, dass ebenso die Managementseite betrachtet werden muss. Das Management macht nicht nur steuernde Vorgaben für den Betrieb. Vielmehr ist eine Verzahnung von Management und Betrieb eine Voraussetzung für eine anforderungsgerechte IT-Dokumentation. Letztlich ist die IT-Dokumentation die Informationsbasis für alle Managementent-

scheidungen. Daher haben wir der IT-Managementdokumentation in dieser Auflage ebenfalls ein gesondertes Kapitel gewidmet.

Um bei aller Schwerpunktsetzung ein abgerundetes Fachbuch zur IT-Dokumentation zu präsentieren, haben wir an der bewährten Grundstruktur aus den letzten Auflagen festgehalten und die folgenden Kernthemen in einem oder mehreren Kapiteln beschrieben.

1. Abgrenzung IT-Dokumentation
2. Anforderungen an die IT-Dokumentation
3. IT-Managementdokumentation
4. Dokumentation des IT-Betriebs
 - System-/Infrastrukturbetrieb
 - Aufgaben der operativen Serviceerbringung
5. Anwendungsbetrieb und Anwendungsentwicklung
6. Informationssicherheit, Datenschutz, Notfall
7. Umsetzung in der Praxis

Bei den Recherchearbeiten zur Erstellung des Buchs hat es neben der Aktualisierung vorhandener und der Erarbeitung neuer Themen (s. o.) eine Vielzahl von weiteren Informationen gegeben, die mehr oder weniger direkt auch das Thema IT-Dokumentation betreffen. Diese im Einzelnen in den jeweiligen Kapiteln zu beschreiben, hätte sowohl unsere zur Verfügung stehende Zeit als auch den Rahmen des Buchs gesprengt. Da sie nach unserer Auffassung aber für den ein oder anderen für IT-Dokumentation Zuständigen eine hilfreiche Unterstützung bieten können, haben wir diese Quellen (Normen, Standards, Best Practices) in einer thematisch sortierten Tabelle zusammengefasst und erläutert. Zusammen mit dem Glossar sowie den Tipps zum Umgang mit Office-Dokumenten ergab sich daraus ein gesondertes Kapitel „Wissenswertes zum Nachschlagen“.

Wir freuen uns auf Ihr Feedback und auf einen regen Gedankenaustausch, auch zu unserem Blog „itdoku-kompakt“ (<https://itdoku-kompakt.de/>)!

Ihre Autoren

Manuela und Georg Reiss



- Wenn bei personellen Bezeichnungen die männliche Form gewählt wurde (z. B. Mitarbeiter, Administrator), so sind damit in gleicher Weise weibliche Mitarbeiter oder Transgender-Mitarbeiter gemeint.
- Wenn in diesem Buch von Unternehmen die Rede ist, sind damit in gleicher Weise auch andere Organisationen wie Behörden, Körperschaften usw. gemeint.

Inhalt

Vorwort	XIII
1 IT-Dokumentation – was ist das?	1
1.1 Zusammenfassung	1
1.2 Nutzergruppen und deren Anforderungen an die Dokumentation	1
1.3 Scoping der IT-Dokumentation	3
1.3.1 Mögliche Strukturierungsansätze für die IT-Dokumentation	3
1.3.2 Festlegung der Strukturierungssicht	4
1.3.3 Dokumentation aus Sicht des IT-Managements	7
1.4 Zusammenspiel des aktuellen Ansatzes mit der Strukturierung vorhergehender Auflagen	10
2 Anforderungen an die IT-Dokumentation	13
2.1 Zusammenfassung	13
2.2 Compliance-Anforderungen identifizieren	14
2.3 Rechtliche Regelwerke mit Relevanz für die IT-Dokumentation	16
2.3.1 Handelsgesetzbuch (HGB) und Abgabenordnung (AO)	16
2.3.2 Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	18
2.3.3 Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG-neu)	21
2.3.4 Telemediengesetz (TMG)	23
2.4 Anforderungen aus branchenspezifischen Vorschriften	25
2.4.1 IT-Sicherheitsgesetz	25
2.4.2 Energiewirtschaftsgesetz (EnWG)	27
2.4.3 Compliance-Anforderungen der Chemie-, Pharma-, Gesundheits- und Lebensmittelbranche	28
2.4.4 Compliance-Anforderungen für Finanzdienstleister	29
2.4.4.1 Mindestanforderungen an das Risikomanagementsystem (MaRisk)	30

2.4.4.2	Mindestanforderungen an die Sicherheit von Internetzahlungen – MaSI	32
2.4.4.3	Bankaufsichtliche Anforderungen an die IT – BAIT	33
2.5	Normen und Standards	34
2.5.1	Normierungsorganisationen	35
2.5.2	Standardisierung der ISO-Normen	37
2.6	Was prüfen Wirtschaftsprüfer und Revisoren?	38
2.6.1	Jahresabschlussprüfung	39
2.6.2	Prüfungen durch die Revision	42
2.6.3	Prüfung der Verfahrensdokumentation	44
2.6.3.1	Aufbau und Inhalt einer Verfahrensdokumentation	45
2.6.3.2	Formale Anforderungen an die Verfahrensdokumentation	47
3	Dokumentation für das IT-Management	49
3.1	Zusammenfassung	49
3.2	Handlungsfelder des IT-Managements	49
3.2.1	Identifizierung der relevanten IT-Managementbereiche	50
3.2.2	Dokumentationsanforderungen festlegen	53
3.3	Aufbau einer an IT-Services und IT-Prozessen ausgerichteten Dokumentation ..	58
3.3.1	Standards für das IT-Servicemanagement	60
3.3.2	Stufenmodell für die IT-Dokumentation	62
3.3.2.1	Einführung in das Stufenmodell	62
3.3.2.2	Stufenbezogene Dokumentationsanforderungen	65
3.3.2.3	„Gebrauchsanweisung“ für die Nutzung des Stufenmodells	68
3.4	Wichtige Dokumente des IT-Servicemanagements	73
3.4.1	Servicebeschreibungen (SLAs)	73
3.4.2	Servicekatalog	74
3.4.3	Leistungsscheine	76
3.4.4	Prozessbeschreibungen	77
3.4.4.1	Inhalte einer Prozessbeschreibung	78
3.4.4.2	Prozesssteckbrief	79
3.4.4.3	Grafische Prozessbeschreibungen	81
3.4.4.4	Grundlegende Empfehlungen für die Prozessdokumentation	88
3.4.5	Prozesslandkarte zur Darstellung der Verzahnung von Fachbereichen und IT	89
3.4.6	Rollenkonzept	91
3.4.7	Betriebsmatrix	95
4	Dokumentation für den IT-Betrieb	97
4.1	Zusammenfassung	97
4.2	Aufbau der IT-Betriebsdokumentation	97
4.3	IT-System-/Infrastrukturbetrieb	99
4.3.1	Aufbau der Systemdokumentation	100
4.3.2	Strukturierung der Systemakten	102
4.3.2.1	IT-Systeme	105

4.3.2.2	Anwendungen	109
4.3.2.3	Netzwerkkomponenten	113
4.3.2.4	Infrastruktur	113
4.3.2.5	Industrielle IT	116
4.3.3	Festlegung der Systemakteninhalte	117
4.3.4	Dokumentation der operativen Tätigkeiten	123
4.3.4.1	Strukturierung der operativen Tätigkeiten	123
4.3.4.2	Operative Tätigkeiten sind keine Prozesse	126
4.3.4.3	Ablaufbeschreibungen	127
4.3.4.4	Arbeitsanleitungen und Arbeitsanweisungen	128
4.3.5	Umsetzungsbeispiele für die Verwaltung von Systemakten	133
4.3.5.1	Automatisierte Inventarisierung	133
4.3.5.2	Dokumentation von Systemabhängigkeiten in einer CMDB	134
4.3.5.3	Berechtigungskonzept	134
4.3.5.4	Berechtigungsmatrix	135
4.4	Dokumentation für die Funktionen der IT-Serviceerbringung	137
4.4.1	ITIL® im Überblick	137
4.4.1.1	„Typischer“ Ablauf einer ITIL®-Einführung	139
4.4.1.2	Der Service Lifecycle im Überblick	142
4.4.2	Dokumentation der IT-Service-Management-Prozesse	144
4.4.2.1	Strukturierung der Prozesse	144
4.4.2.2	Dokumente der operativen Serviceerbringung	145
4.4.2.3	Management der IT-Assets	153
4.4.3	Es muss nicht immer ITIL® sein	155
5	Anwendungsentwicklung und Anwendungsbetrieb	157
5.1	Zusammenfassung	157
5.2	Was gehört zur Anwendungsdokumentation?	157
5.2.1	Anwendungsklassifizierung	159
5.2.2	Abgrenzung zur Softwaredokumentation	161
5.2.3	Abgrenzung zur Verfahrensdokumentation	163
5.2.4	Dokumentation im Rahmen des Application Lifecycle Management	164
5.3	Wesentliche Ergebnistypen im Softwareentwicklungsprozess	166
5.3.1	Anforderungsdokumente – Lastenheft und Fachkonzept	167
5.3.2	Designdokumente	172
5.3.3	Testdokumente	177
5.3.4	Betriebsdokumente	181
5.3.5	Dokumentenübergabe an den Betrieb	184
5.3.6	Dokumentation bei agiler Softwareentwicklung	185
5.4	Dokumentation für das Projektmanagement	187
5.4.1	Bestandteile der Projektdokumentation	188
5.4.1.1	Projektmanagement-Handbuch	190
5.4.1.2	Projektakten	192
5.4.1.3	Prozesse im Projektmanagement	194
5.4.2	Anforderungsgerechte Projektmanagementdokumentation	201
5.4.2.1	Phasen- und prozessorientierte Dokumentenstruktur	204

5.4.2.1.1	Projektphasen	204
5.4.2.1.2	Projektmanagementphasen	205
5.4.2.2	Strukturierung der Projektmanagementdokumente	206
5.4.3	Organisation der Projektdokumentation	207
5.4.3.1	Dokumentationsstandards auch für Projekte	208
5.4.3.2	Problemfeld Dokumentenverwaltung im Projekt	209
6	Informationssicherheit, Notfallmanagement und Datenschutz	213
6.1	Zusammenfassung	213
6.2	Dokumentation für das Informationssicherheitsmanagement	213
6.2.1	Regulierien für die Informationssicherheit	215
6.2.1.1	ISO 27001	216
6.2.1.2	IT-Grundschutz des BSI	217
6.2.1.3	Handbuch Wirtschaftsgrundschutz	219
6.2.2	Aufbau der ISMS-Dokumentation	221
6.2.2.1	ISO 27001 Dokumentation	221
6.2.2.1.1	Erforderliche Dokumente zur Steuerung des Informationssicherheitsprozesses	222
6.2.2.1.2	Dokumentation zur Umsetzung der Maßnahmen	223
6.2.2.1.3	Nachweisdokumente	224
6.2.2.2	IT-Grundschutzdokumentation	225
6.2.2.2.1	Erforderliche Dokumente und deren Zuordnung	226
6.2.2.2.2	Prozessbausteine als Strukturierungsansatz für die managementbezogenen ISMS-Dokumente	226
6.2.2.3	Leitlinie und Konzept für die Informationssicherheit	231
6.2.2.3.1	Inhalte einer Leitlinie	231
6.2.2.3.2	Inhalte eines Sicherheitskonzepts	232
6.3	Dokumentation für den Datenschutz	237
6.3.1	Dokumentationspflichten gemäß DSGVO	238
6.3.2	Verzeichnis der Verarbeitungstätigkeiten	243
6.3.3	Dokumentationspflichten für IT-Organisationen	245
6.3.4	Dokumentation bei Auftragsverarbeitung	249
6.4	Dokumentation für den Notfall	251
6.4.1	Notfallrelevante Standards im Überblick	252
6.4.1.1	BSI-Standard 100-4	252
6.4.1.2	Standards und Normen der British Standards Institution	255
6.4.1.3	ISO 22301 und ISO 22313	256
6.4.1.4	ISO-27000-Normenfamilie	256
6.4.1.5	Good Practice Guidelines	257
6.4.1.6	ISO 20000	257
6.4.2	Die Rolle der IT im unternehmensweiten Notfallmanagement	258
6.4.3	Dokumente für die Notfallvorsorge	262
6.4.3.1	BIA und Risikoanalyse bilden die Basis	263
6.4.3.2	Notfallvorsorgekonzept	265
6.4.3.3	Notfallvorsorge aus Sicht von IT-Service Continuity Management	267

6.4.4	Dokumentation für die Notfallbewältigung	269
6.4.4.1	Strukturierung des Notfallhandbuchs	270
6.4.4.2	Notfallorganisation	270
6.4.4.3	Sofortmaßnahmen	272
6.4.4.4	Notfallbewältigung	272
6.4.4.5	Ergänzende Pläne	275
6.4.4.6	Kommunikationspläne	275
6.4.4.7	Geschäftsführungspläne	276
6.4.4.8	Wiederanlaufpläne	276
6.4.4.9	Wiederherstellungspläne	278
6.4.4.10	IT-Notfallhandbuch	278
6.4.5	Test- und Übungsdokumentation	281
6.4.6	Umsetzungsrahmenwerk (UMRA) zum Notfallmanagement	284
6.4.7	Tool-Unterstützung für die Falldokumentation	286
7	Umsetzung in der Praxis	287
7.1	Zusammenfassung	287
7.2	Ohne Dokumentationsmanagement funktioniert es nicht	287
7.3	Managementrahmen für die Dokumentation	290
7.3.1	Dokumentationsrichtlinie	291
7.3.1.1	Regelungen zur Qualitätssicherung	292
7.3.1.2	Verantwortlichkeiten	292
7.3.1.3	Dokumentationsverfahren	293
7.3.1.4	Allgemeingültige Regelungen	293
7.3.2	Dokumentationskonzept	293
7.3.2.1	Dokumentenklassen und Dokumententypen	294
7.3.2.2	Festlegungen für die Dokumentenablage	296
7.3.2.3	Kennzeichnungspflichten für Vorgabedokumente	296
7.3.2.4	Formale Vorgaben	299
7.3.3	Glossar	300
7.3.4	Namenskonventionen	300
7.4	Zu lenkende Dokumente der IT-Dokumentation	301
7.5	Dokumentenverwaltung	301
7.5.1	Regelungen für Dokumente	302
7.5.2	Regelungen für Aufzeichnungen	306
7.6	Anwendungen für die Dokumentation und dokumentationsrelevante Anwendungen	307
7.6.1	Die Suche nach der „Eierlegenden Wollmilchsau“	308
7.6.2	Anwendungen für die Dokumentation	310
7.6.2.1	Planung des DMS ist elementar	313
7.6.2.2	Rechtliche Aspekte beim DMS-Einsatz	314
7.6.3	Anwendungen mit Relevanz für die IT-Dokumentation	316
7.6.3.1	Systemdokumentation	316
7.6.3.2	Prozessdokumentation	317
7.6.3.3	IT-Servicemanagementdokumentation	318
7.6.3.4	ISMS-Dokumentation	323

7.6.3.5	Notfalldokumentation	323
7.6.3.6	GRC-Dokumentation	325
7.7	Aufbau einer Website für die IT-Dokumentation am Beispiel von SharePoint	326
7.7.1	Planung der Umsetzung	327
7.7.1.1	Websitestructur	328
7.7.1.2	Rollen und Berechtigungen	329
7.7.1.3	Inhaltsverwaltung	330
7.7.1.4	Planung der Dokumentensteuerung	333
7.7.2	Einrichtung eines WIKIs zur Verwaltung von Anwendungshandbüchern	336
7.7.3	Inhalte eines DMS-Konzepts	339
7.8	Organisation der Dokumentenerstellung	340
7.8.1	Vom leeren Blatt zum fertigen Dokument	341
7.8.2	Planung und Vorbereitung	341
7.8.3	Recherche und Aufbereitung von Informationen	342
7.8.4	Vorgaben und Dokumentenumfeld klären	343
7.8.5	Richtiges Vorgehen bei der Dokumentenerstellung	345
7.8.6	Checkliste für die Qualitätssicherung	347
8	Wissenswertes zum Nachschlagen	351
8.1	Zusammenfassung	351
8.2	Glossar	351
8.3	Weitere Normen, Standards, Empfehlungen	362
8.3.1	Bereich Arbeitsschutz	362
8.3.2	Bereich Archivierung	362
8.3.3	Bereich Audits und Assessments	363
8.3.4	Bereich Barrierefreiheit	367
8.3.5	Bereich Datenschutz	368
8.3.6	Bereich Dokumentation	370
8.3.7	Bereich Informationssicherheit	371
8.3.8	Bereich Internes Kontrollsystem	380
8.3.9	Bereich IT-Governance	383
8.3.10	Bereich IT-Beschaffung	384
8.3.11	Bereich IT-Servicemanagement	386
8.3.12	Bereich IT-Strategie	388
8.3.13	Bereich IT-Systemarchitekturen	388
8.3.14	Bereich Notfallmanagement	389
8.3.15	Bereich Projektmanagement	392
8.3.16	Bereich Qualitätsmanagement	395
8.3.17	Bereich Risikomanagement	396
8.3.18	Bereich Softwareentwicklung	398
8.3.19	Bereich Wirtschaftsprüfung	402
8.4	Dokumente erstellen mit Office und Co.	403
8.4.1	Microsoft Word optimal nutzen	403
8.4.1.1	Wichtige Funktionen im Backstage-Bereich	404
8.4.1.2	Formatvorlagen erleichtern die Standardisierung	410

8.4.1.3	Die Verzeichnisfunktionen richtig nutzen	415
8.4.1.4	Daten aus anderen Anwendungen einfügen	423
8.4.2	Nützliche Helfer für die Dokumentenerstellung	427
8.4.2.1	Dokumentationsunterstützung mit Mindjet MindManager	428
8.4.2.2	Snagit	433
8.4.2.3	Adobe Acrobat	436
9	Abkürzungen, Literatur und Gesetze/Verordnungen	441
9.1	Abkürzungsverzeichnis	441
9.2	Literaturnachweise	445
9.3	Gesetze und Verordnungen	448
Index	451

3

Dokumentation für das IT-Management

■ 3.1 Zusammenfassung

Nicht nur, weil in dem Buch ein managementbezogener Strukturierungsansatz für die IT-Dokumentation verwendet wird, sondern auch aufgrund der steuernden Aufgaben und der Verantwortlichkeit der Entwicklung von Vorgaben für den IT-Betrieb wird in diesem Kapitel die Dokumentation für das IT-Management beschrieben.

Die Inhalte und der Umfang der Dokumentation für das IT-Management hängen sehr stark davon ab, wie sehr sich die IT-Organisation serviceorientiert aufgestellt hat. Das reicht von Organisationen, die fast ausschließlich operativen IT-Betrieb durchführen, bis hin zu IT-Organisationen, die ITIL® vollumfänglich umsetzen und ihre Organisation entsprechend ausgerichtet haben. Daher wird im Managementkapitel ein Stufenmodell dargestellt, das fünf Stufen der Serviceorientierung beschreibt. IT-Organisationen können daraus ableiten, welchen Umfang die Managementdokumentation haben sollte. Dies ist selbstverständlich ein Modellvorschlag. Die konkrete Festlegung muss jede IT-Organisation letztlich selbst treffen.

Wesentliche Dokumente für das Servicemanagement sind in dem Kapitel genauer vorgestellt worden und bieten eine Grundlage für die mögliche Ausgestaltung der Dokumentation des IT-Managements.

■ 3.2 Handlungsfelder des IT-Managements

Im vorliegenden Praxishandbuch steht die Dokumentation des IT-Betriebs im Fokus. Da aber, nach dem von den Autoren gewählten Ansatz, die Dokumentation der operativen Funktionen maßgeblich durch das Management vorgegeben und gesteuert wird bzw. gesteuert werden sollte, ist eine Betrachtung der Handlungsfelder des IT-Managements und deren Einfluss auf die Dokumentation für den operativen Betrieb unerlässlich.

Nicht nur die in *Kapitel 2* beschriebenen regulatorischen Anforderungen, sondern auch die steigenden Wettbewerbsanforderungen an IT-Abteilungen führen dazu, dass der Erfolgs-

druck auf die CIOs weiter zunimmt. Heute müssen IT-Organisationen jederzeit in der Lage sein, Umstrukturierungen, Fusionen und neue Kooperationsmodelle schnell und sicher zu bewältigen. Themengebiete wie IT-Strategie, IT-Risikomanagement und IT-Compliance gewinnen daher für das IT-Management zunehmend an Relevanz. Außerdem kommen immer wieder neue Managementaufgabengebiete hinzu. Integriertes Management, Datenschutzmanagement und Business Servicemanagement sind nur einige Themen, mit denen sich auch das IT-Management heute auseinandersetzen muss.

Dabei stehen vor allem Fragen zur Einbindung von IT-Governance als Teilbereich der unternehmensweiten (Corporate) Governance und daraus abzuleitenden Entwicklungsmaßnahmen im Fokus. IT-Governance umfasst Organisationsstrukturen und Prozesse, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele wirksam unterstützt. Die Reduzierung möglicher Risiken sowie Gesetzes- und Regelkonformität (IT-Compliance) sind dabei die wesentlichen Steuerungsziele.

Und mit jeder neuen Anforderung nehmen auch die Dokumentationsaufgaben zu. Denn keiner der genannten Managementansätze ist eine Einmalaufgabe, sondern erfordert vielmehr einen kontinuierlichen Verbesserungsprozess sowie ein *internes Kontrollsystem (IKS)* mit steigender Effektivität. Beides aber ist ohne eine anforderungsgerechte Dokumentation nicht umsetzbar.

3.2.1 Identifizierung der relevanten IT-Managementbereiche

Im Rahmen des Aufbaus einer ganzheitlichen IT-Dokumentation müssen im ersten Schritt die Dokumentationsanforderungen aller für die IT-Organisation relevanten Managementfunktionen identifiziert werden. Hierzu ist es erforderlich, zuvor den Gesamtrahmen der IT-Managementdokumentation abzustecken.

Konkret bedeutet dies, festzustellen, welche Managementfunktionen es in der IT-Organisation gibt, die im Rahmen der IT-Dokumentation zu berücksichtigen sind. Eine Hilfestellung kann dabei die nachstehende Übersicht der möglichen Management-Aufgabenfelder bieten. Diese basieren auf dem von BEETZ [2014] veröffentlichten Modell der IT-Governance-Prozesse.

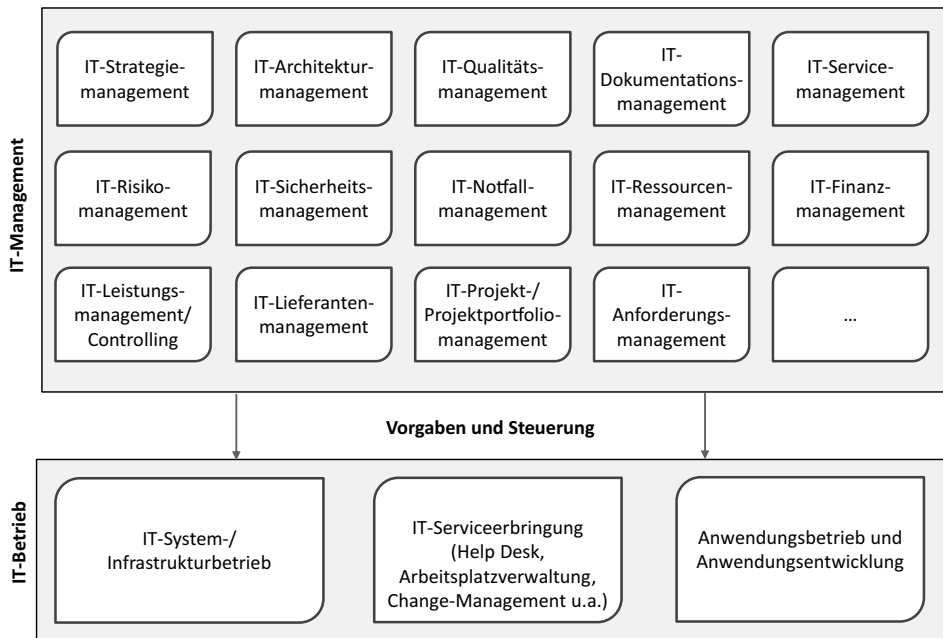


Bild 3.1 Aufgabenfelder der IT-Organisation. Quelle: In Anlehnung an Reiss [2018]

Die dargestellten Aufgabenfelder sind exemplarisch und erheben keinen Anspruch auf Vollständigkeit, da diese vom Zuschnitt der IT-Organisation im Unternehmen abhängen. Außerdem ist zu beachten, dass die Bereiche in der Praxis häufig nicht überschneidungsfrei voneinander zu trennen sind, stattdessen gibt es viele Überlagerungen und Schnittstellen. In der Konsequenz existieren auch bei der Dokumentation Überschneidungsbereiche, die unternehmensspezifisch zu regeln sind. So kann die Pflege der Prozessdokumentation dem zentralen Qualitätsmanagement oder einer eigens dafür eingesetzten Stelle als Aufgabe zugeordnet sein. In der Folge werden die IT-Prozesse dann auch nicht durch die IT-Organisation, sondern durch eine zentrale Stelle dokumentiert und veröffentlicht.

Und auch eine Erweiterung der Aufgabenfelder kann notwendig sein. Abhängig vom Reifegrad des IT-Service-Managements ist beispielsweise eine Ausweisung der in ITIL® verwendeten Phasen *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* als eigenständige Handlungsfelder sinnvoll (siehe hierzu *Kapitel 4, Abschnitt 4.4*).



MindMaps zur Erarbeitung einer Dokumentationsstruktur

Bei der Planung der Dokumentationsstruktur für die IT-Organisation ist es sinnvoll, diese grafisch zu veranschaulichen. MindMaps sind hierfür ein gutes Werkzeug. Sie können sowohl zur gemeinsamen Erarbeitung in Workshops als auch zur Dokumentation der Dokumentenstrukturen verwendet werden.



Bild 3.2 Festlegung der einzubeziehenden IT-Managementbereiche im MindMap

3.2.2 Dokumentationsanforderungen festlegen

Sind die für die Dokumentation relevanten Handlungsfelder benannt, sollten im nächsten Schritt die Dokumentationsanforderungen einschließlich der in „in jedem Fall“ benötigten Dokumente für die einzelnen jeweiligen Handlungsfelder festgelegt werden.

Für einzelne Handlungsfelder wie dem Strategiemanagement beispielsweise lässt sich diese Aufgabe sicherlich recht einfach lösen. Für andere Bereiche wie dem IT-Service-management oder dem IT-Sicherheitsmanagement sind die Dokumentationsanforderungen nicht so eindeutig. Für diese Bereiche kann das von den Autoren entwickelte und in *Abschnitt 3.3.2* vorgestellte Stufenmodell für die IT-Dokumentation hilfreich sein. Dieses soll dem IT-Management helfen, sich über die für die eigene IT-Organisation bestehenden Dokumentationsanforderungen vor allem für die Bereiche Prozess- und IT-Service-management einen Überblick zu verschaffen.

Für den Bereich IT-Strategiemanagement beispielsweise benennt REISS [2018] die nachstehend genannten Dokumente als üblicherweise vom IT-Strategiemanagement zu pflegenden Dokumente. Wie das nachstehende Beispiel zeigt, ist es sinnvoll, sowohl die Vorgabedokumente wie Richtlinien und Prozessbeschreibungen festzulegen als auch die wichtigsten Nachweisdokumente.



Beispieldokumente IT-Strategiemanagement

Aufgabe des IT-Strategiemanagements ist es, ausgehend vom Ist-Zustand die Vision, Mission, Ziele und Wege, wie die IT zukünftig im Unternehmen genutzt und dafür ausgestaltet sein soll, zu beschreiben. Typische Dokumente sind:

- IT-Strategierichtlinie
- Beschreibung des Strategieprozesses einschließlich Arbeitsanweisungen
- Prozessbeschreibung zur Ermittlung rechtlicher und vertraglicher Anforderungen
- IT-Konzept
- Kennzahlen und Controlling-Ergebnisse
- SWOT- und Gap-Analyse-Darstellungen
- Definition von Rahmenbedingungen für IT-Infrastruktur und Standards
- Nachweise über Abnahme, Veröffentlichung, Überwachung und Review der IT-Strategie, Kennzahlen und Controlling-Berichte

Beispiel IT-Konzept

Ein wichtiges Dokument des Strategiemanagements ist, im Verständnis der Autoren, das IT-Konzept. In der Praxis wird der Begriff jedoch unterschiedlich verwendet, weshalb an dieser Stelle ein paar Ausführungen dazu sinnvoll sind.

Häufig wird der Begriff „*IT-Konzept*“ anstelle des Begriffs „*DV-Konzept*“ verwendet. Demnach handelt es sich bei IT-Konzepten, die dem Anforderungsmanagement zuzuordnen sind und die fachlichen Anforderungen an eine geplante Lösung beschreiben. Im Buch wird hierfür

ausschließlich der Begriff *DV-Konzept* verwendet. Hingegen ist das IT-Konzept als ein singuläres strategisches Dokument definiert, das die Ausrichtung der IT auf die Unternehmensstrategie beschreibt. So wird typischerweise im IT-Konzept festgelegt, ob die IT zentral oder dezentral strukturiert (Fertigungstiefe) ist und mit welcher Ausprägung. Weiterhin sollte das IT-Konzept regeln, mit welchen Verfahren (z. B. nach welchen Standards) das Unternehmen bzw. die IT-Organisation welche Zwecke verfolgt. Damit kann es einen Orientierungsrahmen für die weitere Entwicklung und geplante Maßnahmen aufzeigen. Was im IT-Konzept letztendlich geregelt wird, liegt allein in der Verantwortung der Organisation. So kann ein IT-Konzept durchaus auch Festlegungen (Methoden und Verfahren) zur Einordnung von IT-Projekten beinhalten. Wichtig ist aber, dass es keine Details beschreibt, sondern nur grundsätzliche Regelungen festschreibt, ohne diese zu spezifizieren. Die nachstehende Liste zeigt exemplarisch mögliche Inhalte eines IT-Konzepts:

- Allgemeines
 - Grundsätze
 - Zielsetzung
 - Anforderungen aus gesetzlichen Vorschriften
 - Abgrenzung zu anderen IT-Richtlinien
 - Geltungsbereich
- Organisation
 - Verantwortliche Bereiche
 - Struktur (Organigramm)
- Verantwortung
 - Aufgabenbereiche
 - Rollen
 - Kompetenzen
 - Zentrale IT-Dienstleister
 - Entscheidungs pyramid

Hinsichtlich der Rollenbeschreibungen kann es sinnvoll sein, im IT-Konzept die High-Level-Rollen zu definieren. Dies ersetzt jedoch nicht das in *Abschnitt 3.4.6* beschriebene Rollenkonzept für die Betriebsrollen. Mögliche Rollendefinitionen für den operativen Anwendungsbetrieb können beispielsweise folgendermaßen aussehen:

- **Systemadministratoren:** Systemadministratoren installieren, konfigurieren und betreiben IT-Systeme. Der ordnungsgemäße Betrieb der IT-Systeme beinhaltet die Einhaltung der vereinbarten Verfügbarkeitsanforderungen, die Datenschutzvereinbarungen sowie die Anwendung und Einhaltung der jeweiligen Sicherheitsrichtlinien. Systemadministratoren haben die erforderlichen Qualifikationen für die Systemumgebung nachzuweisen.
- **Anwenderbetreuer:** Anwenderbetreuer bilden die Schnittstelle zwischen den Administratoren und dem Anwender. Sie nehmen Leistungen des Supports wahr und bereiten die Serviceanfragen und Störungsmeldungen der Nutzer systematisch auf. Können Probleme nicht vor Ort gelöst werden, organisieren und überwachen Anwenderbetreuer die Problemeskalation und -lösung. Außerdem übernehmen sie Schulungsaufgaben in der unmittelbaren Anwenderumgebung.

- **Anwendungsadministratoren:** Applikationen werden von den jeweiligen Administratoren konfiguriert und gewartet. Sie entwerfen Berechtigungskonzepte und setzen diese in der Benutzerverwaltung um. Die administrative und technische Betreuung erfolgt in enger Verbindung zur System- und Datenbankadministration. Änderungserfordernisse, die nicht durch Customizing der Anwendung und/oder des Systems erreicht werden können, sind als Entwicklungsaufgaben an das Change-Management weiterzuleiten.
- **Key-User:** Als Key-User werden Anwender einer Anwendung verstanden, wenn sie über besondere Kenntnisse im Umgang mit und in den Funktionalitäten der Anwendung verfügen. Sie stellen ein Bindeglied zwischen der Anwenderbetreuung und dem „Standard“-Nutzer dar und werden zu Multiplikatoren bei der Verbreitung von Know-how, bezogen auf das jeweilige Verfahren. Sie sind i. d. R. nicht in der IT angesiedelt.

Es ist nicht das Ziel des Buchs, die Dokumentationsanforderungen und erforderlichen Dokumente aller IT-Managementbereiche zu beschreiben. Hier sei auf das ebenfalls von der Autorin veröffentlichte Buch *Dokumentationsmanagement - Basis für IT-Governance: 11 Schritte zur IT-Dokumentation* verwiesen. Exemplarisch werden im nachfolgenden Abschnitt grundsätzliche Dokumentationsanforderungen an eine an IT-Services bzw. IT-Prozessen ausgerichtete IT-Organisation erläutert.

Definition „Verfahren“

In den vorstehenden Ausführungen wurde mehrfach der Begriff „Verfahren“ verwendet. Leider findet man in kaum einem anderen Bereich so viele unterschiedliche Bedeutungen für einen Begriff wie für das Wort „Verfahren“. Umgekehrt gibt es keinen standardisierten Begriff, mit dem allgemeingültig die Dokumentation von Abläufen (z.B. Durchführung mehrstufiger Testläufe) benannt wird. Von Verfahrensbeschreibungen, Ablaufbeschreibungen, Beschreibungen für Fachverfahren bzw. IT-Lösungen, aber auch Konzept reicht die Spannweite und diese Auflistung ist noch längst nicht vollständig. Eine hilfreiche Definition, die auch dem Verständnis der Autoren entspricht, findet sich bei SCHMIDT, BRAND [2011]:

„Ein Fachverfahren ist ein Verfahren in einem Unternehmen, das in einem Fachbereich angewendet wird, um eine fachliche Aufgabe durchzuführen. Fachliche IT-Verfahren sind informationstechnische Verfahren im Unternehmen, die die Fachverfahren technologisch unterstützen. Hierfür findet sich auch der Begriff der IT-Lösung.“

Die folgenden Ausführungen sollen diese Definition verdeutlichen. Bei einer prozessorientiert agierenden IT-Organisation stehen die Geschäftsprozesse im Mittelpunkt der betrieblichen IT-Organisation und der Betrieb erfolgt auf Basis definierter Prozesse. Hierbei wird das gesamte Handeln als eine Kombination von Prozessen betrachtet und Aufgaben werden organisationsübergreifend anhand von in Prozessen beschriebenen Aktivitäten bearbeitet und über Rollendefinitionen den Ressourcen aus den Organisationsbereichen zugeordnet. Ein Verfahren ist ein zusammenhängend ablaufender Teil eines Prozesses, bei dem die operative Sicht im Vordergrund steht. Verfahren stellen demnach operative Detailansichten eines Prozesses dar. Sie können, müssen jedoch nicht IT-unterstützt durchgeführt werden. Während Prozessbeschreibungen (siehe *Abschnitt 3.4.4*) den Prozessablauf strukturiert darstellen und die Abläufe beschreiben, in denen Verfahren abgewickelt werden, stellt eine **Verfahrensbeschreibung** dar, wie ein Prozess operativ auszuführen ist bzw. wie er ein

Ergebnis erzielt. Auch gängige Standards und Normen unterscheiden in diesem Sinne zwischen Prozessen und Verfahren (Verfahrensbeschreibungen werden vielfach auch als *Verfahrensleitungen* oder *Verfahrensanweisungen* bezeichnet).

Aktivitäten bilden die kleinste Ausführungseinheit und sind dadurch gekennzeichnet, dass die Verantwortung für diese nicht unterteilbar ist. Die Durchführung von Aktivitäten sollte durch Arbeitsanleitungen und Ablaufbeschreibungen unterstützt werden.

Arbeitsanleitungen und **Ablaufbeschreibungen** *wiederum* beschreiben im Vergleich zu den Verfahrensbeschreibungen auf einer tieferen Ebene detailliert die einzelnen Aktivitäten. Sie sind an einen Prozess bzw. ein Verfahren gebunden und regeln tätigkeitsbezogene Abläufe. Bei ITIL® findet man diese Dokumente unter der Bezeichnung *Standard operating procedures* – *SOPs*. Damit beschreibt ITIL® ein „Set“ an Dokumenten, die zum einen detaillierte Anleitungen und Zeitpläne für die täglichen Routinearbeiten und zum anderen Anleitungen zur Durchführung von Aktivitäten umfassen.



Beispiel: Prozess – Verfahren – Aktivitäten

Durchführung eines Change (Versionsupdate einer Anwendung)

Prozess: Der hier betrachtete Change-Prozess beinhaltet typischerweise die folgenden Teilprozesse: Change Request prüfen, Change genehmigen, neue Version paketieren und testen, Change freigeben, Rollout der neuen Version, Evaluierung und Abschluss.

Verfahren: Nach der Paketierung durchläuft das Softwarepaket verschiedene Tests. Die Test- und Freigabeverfahren gehören dabei zu den wichtigsten Verfahren eines Change-Prozesses: Systemtest, Integrationstest, Abnahmetest u. a. und Abnahmen.

Aktivitäten: Eine Aktivität bildet die kleinste Einheit in einem Verfahren. Jedes Verfahren besteht aus einer Reihe von Aktivitäten: Testfallfindung, Beschreiben je Testfall, was genau zu testen ist, Festlegen und Erstellen der Eingabedaten, Testdurchführung u. a.

Aus Sicht von Wirtschaftsprüfern werden Verfahren jedoch eingeschränkter definiert. Demnach ist die Verfahrensdokumentation zunächst auf die rechnungslegungsrelevanten Prozesse gerichtet und damit Geschäftsprozessebene. Sie dient hier zum Nachweis, dass die Anforderungen des Handelsgesetzbuchs (HGB), der Abgabenordnung und der GoBS bzw. der GoBD an die Entwicklung und den Betrieb von Anwendungen sowie an die Verarbeitung und die Archivierung der Daten erfüllt sind. So ist beispielsweise ein Unternehmen verpflichtet, seine rechnungsrelevanten Daten revisionssicher zu archivieren und dies auch in der *Verfahrensbeschreibung* zu dokumentieren: von der Entstehung der Information über die Indizierung und Speicherung, das eindeutige Wiederfinden, die Absicherung gegen Verlust und Verfälschung bis zur Reproduktion am Bildschirm und auf dem Drucker. *Kapitel 2, Abschnitt 2.6.3* beschreibt, worauf bei einer GOBD-konformen Verfahrensbeschreibung zu achten ist. Erläutert wird, welche Inhalte erforderlich sind und worauf Revisoren bei der Prüfung der Verfahrensdokumentation Wert legen.

Aufgrund des hohen Durchdringungsgrads der IT in den Unternehmensprozessen sind die IT-Systeme und IT-Abläufe zur Unterstützung der Unternehmensprozesse immer ein Teil der Verfahrensdokumentation. Daher sind einige der im Bereich der IT-Betriebsdokumentation zu erstellenden Dokumente der Verfahrensdokumentation zuzuordnen. Sie stellen jedoch nur einen Teilbereich dar.



Verwendung der Begriffe definieren

Bereits an mehreren Stellen im Buch wurde auf die Notwendigkeit hingewiesen, die Verwendung von Dokumentationsbegriffen für das eigene Unternehmen zu definieren. Die völlig unterschiedliche Verwendung des Begriffs *Verfahren* macht dies noch einmal deutlich. Definieren Sie daher unbedingt in einem Glossar, welche Begriffe Sie in Ihrem Unternehmen für welche Dokumente bzw. Dokumentationsbereiche verwenden. Die Erstellung eines Konzepts für die Dokumentation sowie eines Glossars ist hierbei hilfreich (siehe hierzu die Ausführungen in *Kapitel 7*).

Dokumente, Aufzeichnungen und dokumentierte Informationen

Unabhängig von der Stufe muss die IT-Organisation sicherstellen, dass das Service-Management-System nachvollziehbar ist und bleibt. Dazu sind *Dokumente* und *Nachweisdokumente* (auch als *Aufzeichnungen* bezeichnet) notwendig, nicht nur aus Compliance-Gründen, sondern auch im Hinblick auf eine anforderungsgerechte effiziente Steuerung der Organisation.

Was ist der Unterschied zwischen einem Dokument und einer Aufzeichnung?

- **Dokumente** (englisch Documents) sind veränderbar. Sie unterliegen formalen Anforderungen und müssen revisorische Anforderungen an Nachvollziehbarkeit, Vollständigkeit, Aktualität und Richtigkeit erfüllen. Dokumente können in einem papierbasierten oder elektronischen Format vorliegen. Typische Dokumente sind Konzepte, Prozessbeschreibungen, Richtlinien dokumente, Handbücher, Leistungsscheine u. a.
- **Aufzeichnungen** (englisch Records) stellen als Nachweisdokumente einen speziellen Dokumententyp dar. Sie entstehen im Rahmen der Serviceerbringung und beschreiben erreichte Ergebnisse. Sie dienen der Nachweispflicht für eine ordnungsgemäße Geschäftsführung und der Einhaltung von Anforderungen. Da Aufzeichnungen per Definition nach deren Erstellung nicht verändert werden, gibt es für diese keine Revisionsstände. Typischerweise zählen Systemprotokolle, Auswertungen (Reports, Analysen, Statistiken), Protokolle (Testprotokolle, Abnahmeprotokolle u. a.), ausgefüllte Formulare und Checklisten zu den Aufzeichnungen.

Zusätzlich hat die ISO/IEC zum Zwecke der Vereinfachung mit ihren als ISO/IEC Directives Part 1 veröffentlichten Richtlinien zur Entwicklung von internationalen Managementsystemnormen den Begriff „*Dokumentierte Informationen*“ (engl. Documented Information) eingeführt. Hierbei handelt es sich um

„information required to be controlled and maintained by an organization (3.01) and the medium on which it is contained. Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer

to – the management system (3.04) including related processes (3.12); – information created in order for the organization to operate (documentation); – evidence of results achieved (records).“ [ISO/IEC Directives Part 1, Annex SL, Appendix 2 Abschn. 3.11, 2018].

Demnach umfassen die dokumentierten Informationen die aus Sicht der jeweiligen Managementnorm vom Unternehmen zu erhebenden und zu lenkenden Informationen (sowohl für das Managementsystem als auch für den Betrieb der Organisation). Sie stellen damit den Teil einer Dokumentation dar, der einer Lenkung zu unterwerfen ist. Ob der Ansatz der ISO allerdings hilft, mehr Klarheit in die Begriffswelt zu bringen, ist fraglich. Zumal für die Unterscheidung von Dokumenten und Nachweisen nun noch zwei weitere Begriffe hinzugekommen sind. Geht es der ISO-Norm um dokumentierte Vorgaben (nach bisherigem Normverständnis *Dokumente*), wird vom „*Aufrechterhalten der dokumentierten Information*“ gesprochen. Werden jedoch Nachweise verlangt (im bisherigen Verständnis der ISO-Normen *Aufzeichnungen*), wird dies als eine „*Anforderung zur Aufbewahrung dokumentierter Information*“ bezeichnet. Hinzu kommt, dass einzelne ISO-Normen selbst die Verbindlichkeit dieser Terminologie aufheben, wie das Beispiel der ISO 9001:2015 zeigt: „*Die Organisationen können die Benennungen verwenden, die für ihre Abläufe am besten geeignet sind (z. B. die Verwendung von ‚Aufzeichnungen‘, ‚Dokumentation‘ oder ‚Protokolle‘ anstatt ‚dokumentierte Informationen‘.*“ [ISO 9001:2015]

■ 3.3 Aufbau einer an IT-Services und IT-Prozessen ausgerichteten Dokumentation

Die IT-Abteilungen in vielen Unternehmen konzentrierten sich lange Zeit auf die Bereitstellung von Hardwaresystemen und Anwendungen sowie auf die Produktion von Softwareanwendungen, bis sich in den späten 1980er-Jahren ein Wandel hin zu Serviceorientierung vollzog. Heute sind IT-Organisationen immer häufiger in der Pflicht, sich als interne Service-Provider aufzustellen, die ihren internen Kunden vertraglich geregelte Dienstleistungen mit definierten Service Level Agreements (SLAs) anbieten. Kundenorientierung, Serviceorientierung und Prozessorientierung stehen damit zunehmend im Fokus der Tätigkeiten von IT-Organisationen. Ausgangspunkt bei einer serviceorientiert ausgerichteten Arbeitsweise sind die Anforderungen des Kunden, die in Form von anforderungsgerechten IT-Services oder individuellen Projekten in der vom Kunden geforderten Qualität umgesetzt werden müssen. Hierfür ist ein anforderungsgerechter Betrieb der IT-Systeme eine notwendige Voraussetzung. Ein solcher Betrieb wiederum erfordert eine adäquate Ressourcenausstattung auf Basis entsprechender Prozesse, die die Effizienz und Effektivität der Leistungserstellung sicherstellen. Gleichzeitig drängen in immer kürzeren Abständen neue Technologien in den Markt, die von der IT analysiert, evaluiert und bereitgestellt werden müssen. Zusammen mit einer steigenden Abhängigkeit der Geschäftsprozesse von der IT ergeben sich daraus auch zunehmende Anforderungen an die IT-Dokumentation. Diese muss nicht mehr nur die Tätigkeiten des operativen IT-Betriebs unterstützen, sondern auch

die Erbringung der IT-Services sicherstellen. Dies führt letztlich zu der Frage, welche Themen- bzw. Aufgabenbereiche die IT-Dokumentation einschließen soll und wie diese strukturiert werden kann.

Eine zunehmend größere Rolle nimmt daher das *IT-Servicemanagement (ITSM)* mit den damit verbundenen IT-Servicemanagement-Prozessen ein. IT-Servicemanagement bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen (Business Alignment). Hierzu umfasst es alle Maßnahmen und Aktivitäten, um die Qualität und Quantität von IT-Services optimal und zielgerichtet zu planen, zu steuern und zu überwachen. Für diese werden klassischerweise innerhalb eines Service-Katalogs allgemeine Rahmenbedingungen definiert. Die spezifischen Bedingungen eines Service sind Gegenstand entsprechender Service Level Agreements (SLA). Erbracht werden die vereinbarten Services vom operativen IT-Betrieb, die i. d. R. in Leistungsscheinen konkretisiert werden.

Der Begriff „**Service**“ wird dabei aber keineswegs einheitlich verstanden und verwendet. Im Buch wird unter einem *Service* ein Mittel zur Generierung von Nutzen für den Kunden verstanden. Er liefert vereinbarte Ergebnisse, ohne dass die Kunden für die Kosten und Risiken, die durch die Serviceerbringung entstehen, Verantwortung tragen müssen. Und ein *IT-Service* ist gemäß Definition des *IT Service Management Forum (itSMF)*

„eine Dienstleistung, die für einen oder mehrere Kunden von einem IT Service Provider bereitgestellt wird. Ein IT-Service basiert auf dem Einsatz der Informationstechnologie und unterstützt die Geschäftsprozesse des Kunden. Ein IT-Service besteht aus einer Kombination von Personen, Prozessen und Technologien und sollte über ein Service-Level-Agreement (SLA) definiert werden. Eine IT-Dienstleistung wird nach dem Dienstleistungsgedanken als abgeschlossene Einheit ähnlich einem Produkt angeboten“ [itSMF-Glossar].

Gemäß dieser Definition werden zur Erbringung von IT-Services Prozesse, Menschen und Informationstechnologie benötigt. IT-Services beschreiben also Produkte auf Basis konkreter Kundenanforderungen und liefern dem Anwender daher einen messbaren Nutzen. In der Standardisierung der Services liegt ein Schlüssel für die wirtschaftliche Serviceerbringung. Die Serviceanforderungen werden in den beteiligten IT-Prozessen im operativen IT-Betrieb mittels Ressourcen (Informationstechnologie und Menschen) umgesetzt.

Und auch der Begriff „**Prozess**“ wird in der Fachliteratur keineswegs einheitlich definiert. Im Buch wird in Anlehnung an KOCH [2015] unter einem Prozess eine Abfolge von Aktivitäten bzw. Aufgaben verstanden, die zeitlich und logisch aufeinander aufbauen und die einen definierten Input in einen definierten Output überführen. Ergebnisse eines Prozesses können anderen Prozessen zur Verfügung gestellt werden oder wiederum Folgeprozesse auslösen. Wichtige Punkte sind hierbei:

- Prozesse gehen über hierarchische Organisationseinheiten hinweg,
- Prozesse überschreiten häufig Organisationsgrenzen,
- Prozesse unterliegen einer besonderen Bewertung auf Basis von Schlüsselindikatoren (KPI),
- Prozesse unterliegen einem KVP. [Koch, 2015]

3.3.1 Standards für das IT-Servicemanagement

Bei der Frage nach einem Standard für das IT-Servicemanagement lautet die Antwort fast immer ITIL®. ITIL® bietet ein Modell für den Aufbau einer serviceorientierten IT-Organisation und eine Sammlung von Best Practices, die eine mögliche Umsetzung eines IT-Servicemanagements beschreiben und international als De-facto-Standard gelten. Und auch die Autoren lehnen sich bei der Betrachtung der Dokumentationsanforderungen für Services und Prozesse an ITIL® an.

Die ISO-Norm 20000 hingegen wird nur selten genannt, bietet aber gegenüber ITIL® den Vorteil der Zertifizierbarkeit. Bei der ISO 20000 handelt es sich um eine speziell auf das IT-Servicemanagement ausgerichtete Norm. Sie wurde im Jahr 2005 auf der Basis der gleichnamigen britischen Norm BS 15000 veröffentlicht. 2011 wurde die ISO/IEC 20000-1 einem Review unterzogen und dabei grundlegend überarbeitet. Aktuell (Stand 08/2018) wird sie wiederum überarbeitet und kann im Entwurf bezogen werden *ISO/IEC FDIS 20000-1:2018-05 - Entwurf*.

Das Ziel der Norm ISO 20000 ist es, einen gemeinsamen Referenzstandard für alle Unternehmen bereitzustellen, welche die IT-Services für interne oder externe Kunden erbringen. Ein weiteres Ziel besteht in der Förderung einer gemeinsamen Terminologie. Wie die meisten aktuellen Standards ist sie qualitäts- und prozessorientiert ausgerichtet, beschreibt aber weniger das produktbezogene Qualitätsmanagement im Allgemeinen, sondern das IT-Servicemanagement im Besonderen. Die prozessorientierten Festlegungen orientieren sich an den Prozessbeschreibungen gemäß ITIL® und ergänzen diese.

Und es besteht ein wesentlicher formaler Unterschied zu ITIL®. Im Gegensatz zu ITIL®, das keinen Standard darstellt, sind die Prozesse des IT-Servicemanagements nach ISO 20000 international anerkannt zertifizierbar. Die ISO 20000 besteht aktuell aus drei Richtlinien-dokumenten und einer Reihe von Ergänzungen (TR - Technischer Bericht), die laufend erweitert werden.

- ISO/IEC 20000-1:2011 - Informationstechnik - Service Management - Teil 1: Spezifikation für Service Management
- ISO/IEC 20000-2:2012 - Informationstechnik - Service Management - Teil 2: Allgemeine Verfahrensregeln für Service Management
- ISO/IEC 20000-3:2012 - Informationstechnik - Servicemanagement - Teil 3: Richtlinie zur Definition des Anwendungsbereichs und Anwendbarkeit der ISO/IEC 20000-1

Dabei stellt Teil 1 die zwingend erforderlichen Anforderungen dar (*must have*), während Teil 2 und Teil 3 weitere optionale Anforderungen beschreiben (*should have*). Eine ISO 20000-Zertifizierung kann auf einen Kunden, einen IT-Service oder einen Standort des IT-Service-Providers begrenzt werden. Durchgeführt werden die Zertifizierungsaudits durch unabhängige Prüforganisationen.

Wie allen aktuellen Managementansätzen, liegt auch der ISO 20000 das Do-Check-Act-Modell, auch bekannt unter dem Namen PDCA-Modell oder Deming-Cycle, zugrunde. Kernpunkt ist das Verständnis von IT-Servicemanagement als geplanter, gelebter, überwachter und sich kontinuierlich verbessernder Prozess. Grundsätzlich gilt es nachzuweisen, dass ein solcher Prozess implementiert wurde und nachhaltig im Unternehmen gelebt wird.



ISO-Redline

Die ISO/IEC 20000-1:2011 kann auch als Redline-Version bezogen werden. Die ISO-Redline ist eine ergänzende PDF-Datei zur Originalnorm, die nur gemeinsam mit dieser bezogen werden kann. Sie zeigt durch farbliche Hervorhebungen, an welchen Stellen der Norm es gegenüber der Vorgängerausgabe Veränderungen gegeben hat.

Neben den prozessüberwachenden Aufgaben kann das IT-Servicemanagement damit in drei Aufgabenbereiche unterteilt werden:

- Die Definition der IT-Services und das Abschließen der Verträge mit den Kunden.
- Die Erbringung der vereinbarten Dienstleistungen.
- Die Überwachung, Messung und das Reporting für die zur Verfügung gestellten IT-Services.

Und aus allen Aufgabenbereichen leiten sich Dokumentationsanforderungen ab. Für eine Zertifizierung erforderlich sind eine Reihe von Dokumenten und Reports, die die Effektivität und Effizienz des Servicemanagements sowie die Planung, das Handling und die Steuerung der Serviceprozesse belegen, und es ist sicherzustellen, dass das Service-Management-System auditier- und damit nachvollziehbar ist und bleibt. Grundsätzlich erforderlich sind die folgenden Dokumente:

- Richtlinien und Managementpläne,
- Dokumentation der Prozesse und Funktionen,
- Nachweisdokumente (Protokolle, Berichte u. a.).

Dabei sind die in der ISO 20000 genannten Dokumentationsanforderungen implizit Voraussetzung, um die Prozesse nachvollziehbar und prüfbar zu machen. Hierbei wird das gesamte Handeln als eine Kombination von Prozessen betrachtet und Aufgaben werden organisationsübergreifend anhand von in Prozessen beschriebenen Aktivitäten bearbeitet und über Rollendefinitionen den Ressourcen aus den Organisationsbereichen zugeordnet. Alle Prozesse sind jeweils einem Prozessverantwortlichen unterstellt. Dieser ist für das Prozessergebnis verantwortlich und übernimmt die Koordination innerhalb der Prozesse und zwischen diesen.

Hilfreich bei der Ermittlung der geforderten Dokumente für eine Zertifizierung kann die von Advisera 2000 Academy bereitgestellte Liste *Checklist of Mandatory Documentation Required by ISO/IEC 20000-1:2011* sein. Diese kann nach einer Anmeldung kostenlos heruntergeladen werden. Wichtige Referenzdokumente sind u. a.

- IT-Servicemanagement-Strategie
- IT-Servicemanagement-Richtlinie
- Service-Level-Management-Richtlinie
- Liste der Services (Serviceportfolio)
- Support-Modell
- Prozessmanagement-Konzept (siehe *Abschnitte 3.4.4 und 3.4.5*)

- ITSM-Rollenkonzept (siehe *Abschnitt 3.4.6*)
- Service-Katalog (siehe *Abschnitt 3.4.2*)
- Vorlagen für Leistungsscheine (siehe *Abschnitt 3.4.3*)
- Kennzahlen und Controlling-Ergebnisse

3.3.2 Stufenmodell für die IT-Dokumentation

Die IT-Organisation jedes Unternehmens ist individuell und muss daher individuell betrachtet werden. Und bei der Entwicklung in Richtung eines service- und kundenorientierten IT-Betriebs befindet sich jede IT-Organisation auf einem anderen Stück dieses Weges. Eine für alle Unternehmen passende Schablone für „die IT-Dokumentation“ kann es daher nicht geben. Vielmehr benötigt beispielsweise eine IT-Organisation, die prozessorientiert aufgestellt ist, eine Prozessdokumentation, die neben den Prozessbeschreibungen zum Beispiel auch ein Rollenkonzept einschließt. IT-Organisationen, deren Arbeitsweise hingegen überwiegend an den Funktionen und Systemen ausgerichtet ist, benötigen diese nachvollziehbarerweise (noch) nicht. Und eine Dokumentation zum Nachweis der Einhaltung sicherheits-, datenschutz- und notfallrelevanter Anforderungen ist zwar von allen Organisationen zu pflegen, doch ist deren Zuordnung zu einer Stufe wiederum davon abhängig, ob hierzu eigenständige Managementprozesse implementiert sind.

Wie die Erfahrungen aus den vorangegangenen Ausgaben des Praxishandbuchs IT-Dokumentation zeigen, ist es aus den zuvor genannten Gründen schwierig, aus einem komplexen generischen Modell die für das eigene Unternehmen relevanten Dokumente zu identifizieren. Benötigt wird vielmehr ein Modell, das die verschiedenen Ausprägungen berücksichtigt. Zur Umsetzung dieses Ansatzes wurde von den Autoren ein Stufenmodell für die IT-Dokumentation entwickelt. Dieses unterscheidet fünf Stufen, die jeweils unterschiedliche Dokumentationsanforderungen abbilden. Wesentliche Merkmale für die Zuordnung zu einer Stufe sind dabei der Grad der Service- und Prozessorientierung, die Ausgestaltung des Systembetriebs sowie der Umsetzungsgrad des Sicherheits- und Notfallmanagements.

Das Modell unterstützt eine praktikable Adaption an die unternehmenseigenen Gegebenheiten. Sowohl kleine öffentliche bzw. private IT-Organisationen, die nicht oder noch nicht prozessorientiert arbeiten, können einen Ansatz zur Dokumentation ihrer IT finden, als auch Unternehmen mit komplexeren IT-Strukturen. Hierbei werden wesentliche Dokumentationsanforderungen sowohl für Managementprozesse als auch für den IT-Betrieb betrachtet.

3.3.2.1 Einführung in das Stufenmodell

Ziel der Autoren ist es, einen Strukturierungsansatz zu bieten, der den Bedürfnissen der meisten IT-Organisationen trotz ihrer unterschiedlichen Ausprägungen hinsichtlich Prozess- und Serviceorientierung gerecht wird. Wesentliche Merkmale für die Zuordnung zu einer Stufe sind dabei der Grad der Service- und Prozessorientierung einer IT-Organisation. Ziel ist es, einen Strukturierungsansatz zu bieten, der den Bedürfnissen der meisten IT-Organisationen trotz ihrer unterschiedlichen Ausprägungen hinsichtlich Prozess- und Serviceorientierung gerecht wird.

Bevor das von den Autoren entwickelte Stufenmodell vorgestellt wird, ist ein Blick auf existierende Strukturierungsansätze (Reifegradmodelle) sinnvoll. Reifegradmodelle ermöglichen eine Bewertung des Maßes an Zuverlässigkeit, Effizienz und Effektivität eines Prozesses, einer Funktion, einer Organisation etc. [Beims 2014] Sie dienen als Basis für eine Selbstbewertung und ermöglichen eine Standortbestimmung. In den letzten Jahren wurden einige Modelle zur Bestimmung des Prozessreifegrads entwickelt. Zu den bekanntesten gehört CMMI. *CMMI (Capability Maturity Model Integration)* ist der Nachfolger des bereits seit 1987 entwickelten CMM (Capability Maturity Model) und wurde entwickelt für die Reifegradbestimmung von Softwareentwicklungsprozessen. Ein zentraler Bestandteil des CMMI ist ein Modell zur Bestimmung der Prozessreife. Da sich das Modell auch für andere Prozesse als die ursprünglich adressierten Entwicklungsprozesse anwenden lässt, wird dieses Modell bereits seit vielen Jahren als Modell zur Reifegradbestimmung auch im IT-Service-Management eingesetzt. Auch ITIL® beschreibt in seinem Reifegradmodell *Process Maturity Framework (PMF)*, das sich sehr stark an CMMI anlehnt, was notwendig ist, um einen angestrebten Prozessreifegrad zu erreichen.

Allerdings dienen diese Reifegradmodelle dazu, den jeweils erreichten Grad zu beurteilen und daraus Ziele und Maßnahmen für Verbesserungen abzuleiten. Dies spielt an dieser Stelle keine Rolle, da weder eine Beurteilung noch eine Verbesserung von Projekt-, Prozess- oder Servicemanagementprozessen primäres Ziel des Buchs sind.

Das im Folgenden beschriebene Stufenmodell für die IT-Dokumentation lehnt sich zwar an vorhandene Reifegradmodelle an, betrachtet aber ausschließlich deren operativen Aspekte. Es dient zur Bestimmung des eigenen Standorts hinsichtlich mehrerer für die IT-Dokumentation relevanter Bereiche und als Hilfestellung für das IT-Management, eine für eine erreichte Stufe angemessene bzw. aus Compliance-Sicht erforderliche Dokumentation zu implementieren. Hierbei stellen die Dokumentationsanforderungen einer höheren Stufe keine Bewertung gegenüber den Dokumentationsanforderungen einer niedrigeren Stufe dar. Der Ansatz ist vielmehr: „Wenn es in einem Unternehmen keine definierten IT-Services gibt, können sie bzw. müssen sie auch nicht dokumentiert werden.“ Daneben gibt es jedoch auch Bereiche, die in jedem Fall zu dokumentieren sind.

Dieser Ansatz entspricht auch dem Verständnis von regulatorischen Anforderungen wie dem IT-Sicherheitsgesetz oder internationalen Standards, wie dem Informationssicherheitsmanagementsystem nach ISO 27001. Auch hier wird jeweils das Erfordernis von Maßnahmen und damit von Dokumentation an den Erfordernissen des jeweiligen Unternehmens ausgerichtet.

Das hier verwendete Stufenmodell zur Ableitung der Dokumentationsanforderungen basiert auf den in Bild 3.3 dargestellten Bereichen eines IT-Betriebs und deren Abhängigkeiten voneinander.

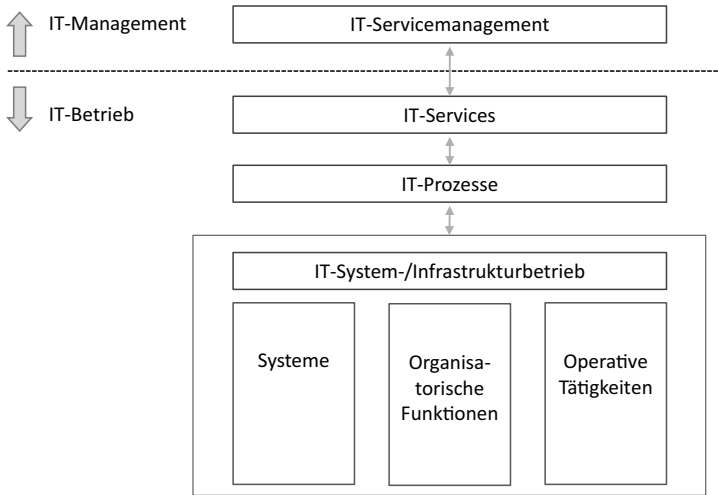


Bild 3.3 Bereiche eines serviceorientierten IT-Betriebs und deren Abhängigkeiten

Zur Ableitung der Stufen werden die Merkmale und deren Ausprägung für die drei Kategorien herangezogen:

- **IT-Services:** In dieser Kategorie wird die Ausprägung des IT-Servicemanagements (ITSM) betrachtet. Die Aufgabe von IT-Servicemanagement ist es, die Qualität und Quantität der IT-Services zu planen, zu überwachen und zu steuern, mit dem übergeordneten Ziel, dass die IT-Services die bestmögliche Unterstützung für die Geschäftsprozesse der internen und externen Kunden bieten. Die Ausprägung von IT-Servicemanagement reicht von einzelnen IT-Services über einen definierten Servicekatalog bis hin zu einem eingeführten und regelmäßig überprüften und verbesserten Service-Management-Prozess gemäß PDCA-Kreis. Dem steht eine IT-Dokumentation gegenüber, die von einzelnen Servicebeschreibungen bis hin zur Abbildung der Services im Rahmen des Service-Lifecycle reicht.
- **IT-Prozesse:** Bei einer prozessorientiert agierenden IT-Organisation erfolgt der Betrieb auf Basis definierter Prozesse sowie standardisierter operativer Tätigkeiten. Hierbei wird der IT-Betrieb als eine Kombination von Prozessen betrachtet und Aufgaben werden organisationsübergreifend anhand von in Prozessen beschriebenen Tätigkeiten bearbeitet und über Rollendefinitionen den Ressourcen aus den Organisationsbereichen zugeordnet. Viele Unternehmen haben zwar Business-Prozesse implementiert und dokumentiert, betrachten aber die IT nach wie vor funktionsorientiert bzw. beziehen die IT-Prozesse nicht mit ein. Dabei spielen IT-Servicemanagement-Prozesse eine wichtige Rolle bei der Umsetzung der Strategie und für das Erreichen der definierten Unternehmensziele. Mittlerweile ist jedoch ein Wandel zu beobachten, d.h., Unternehmen führen Schritt für Schritt auch IT-Prozesse bzw. IT-Servicemanagement-Prozesse ein. Hierbei kann es sich um die Implementierung einzelner Serviceprozesse zur Unterstützung der operativen Tätigkeiten handeln bis hin zu einer prozessorientierten Ausrichtung des gesamten IT-Betriebs.
- **IT-System-/Infrastrukturbetrieb:** Der IT-System-/Infrastrukturbetrieb umfasst den Betrieb der zentralen IT-Komponenten. Dazu gehören u.a. der Betrieb der Serversysteme, die Datensicherung, das Datenbank- und Netzwerkmanagement sowie die Betreuung der

darauf gehosteten Anwendungen. Die Dokumentation beinhaltet alle für den operativen Systembetrieb erforderlichen Dokumente. Es handelt sich hierbei um eine modular aufgebaute Dokumentation, die u. a. alle Dokumente zu dessen Durchführung sowie zu Wartung und Fehlerbehebung beinhaltet. In dieser Kategorie wird auch betrachtet, wie die Tätigkeiten im operativen Betrieb erfolgen (systemorientiert, auf Basis interner operativer Verfahren und Sollvorgaben, proaktiv oder reaktiv u. a.), da dies Auswirkungen auf die Dokumentationsanforderungen hat. Die Dokumentation der Systeme erfolgt in Form von *Systemakten*. Ausführliche Erläuterung zur Strukturierung und zu deren Inhalten finden Sie in *Kapitel 4, Abschnitt 4.2*.

Historisch bedingt sind die genannten Prozessbereiche in der Regel sehr unterschiedlich gut dokumentiert. Während viele technische Abläufe innerhalb der Kernprozesse in sehr vielen Branchen sehr gut beschrieben sind, wurde für die meisten Unterstützungsprozesse eine Dokumentation häufig als nicht erforderlich angesehen. So gibt es wohl kaum einen Produktionsprozess oder eine technische Anlage, für die nicht in irgendeiner Form eine Betriebsanleitung vorliegt. Aber erst mit der immer stärkeren Marktdurchdringung der SAP-Software wurden auch die kaufmännischen Prozesse häufiger dokumentiert. Ähnlich verhält es sich mit den IT-Prozessen. Hier gab und gibt es viele Insellösungen, die bereits sehr gut dokumentiert sind – insbesondere im Mainframe-Bereich. Für andere IT-Bereiche fehlt eine Dokumentation häufig jedoch. Außerdem fokussiert die Dokumentation in aller Regel die Systeme. Ablauf- und Tätigkeitsbeschreibungen sowie eine gesamtheitliche an den Geschäftsprozessen ausgerichtete Dokumentation oder gar die Einbindung der IT-Dokumentation in die Strukturen einer Unternehmensdokumentation sind hingegen eher selten anzutreffen.

Für die Ausführung der Prozesse und damit zur Serviceerbringung werden *Ressourcen* benötigt. Ressourcen für IT-Prozesse sind neben Personen vor allem die IT-Systeme, d.h. Hardware, Software, Netzwerke, Anlagen etc., die für die Entwicklung, Tests, die Bereitstellung, das Monitoring, die Steuerung oder den Support von IT-Services erforderlich sind. In diesem Zusammenhang gilt es noch den Begriff der *Funktion* zu verstehen. Aus der Perspektive von IT-Service-Management handelt es sich bei einer Funktion um

„Ein Team oder eine Gruppe von Personen und die Hilfsmittel, die eingesetzt werden, um einen oder mehrere Prozesse oder Aktivitäten durchzuführen. Ein Beispiel dafür ist das Service Desk.“ [itSMF-Glossar]

3.3.2.2 Stufenbezogene Dokumentationsanforderungen

In Abhängigkeit von der Ausprägung der drei Bereiche *IT-Services*, *IT-Prozesse* und *IT-System-/Infrastrukturbetrieb* werden die folgenden fünf Stufen mit spezifischen Anforderungen an die IT-Dokumentation unterschieden:

- IT-Organisationen der **Stufe 1** agieren überwiegend technologie- und systemgesteuert. Die operativen Tätigkeiten erfolgen anlassbezogen und kaum standardisiert. Auf dieser Stufe sind weder Prozesse noch Services eingeführt und IT-Sicherheit ist ausschließlich systembezogen.
- IT-Organisationen, die sich gemäß dem Stufenmodell der **Stufe 2** zuordnen lassen, agieren per Definition ebenfalls überwiegend technologiegesteuert. Ein wichtiges Merkmal der Stufe 2 ist, dass die Tätigkeiten standardisiert erfolgen und zumindest einzelne Verfahren definiert sind. Oft gibt es besonders in historisch gewachsenen IT-Organisationen

eine Vielzahl von gut eingespielten Abläufen. Allerdings sind diese nur selten ausreichend dokumentiert.

- Die **Stufe 3** ist durch die Einführung von Prozessen gekennzeichnet. Einzelne Aufgaben sind funktionsübergreifend als IT-Prozesse definiert und auch einzelne IT-Servicemanagement-Prozesse sind bereits eingeführt (beispielsweise ein Prozess zum Umgang mit Störungen). Die Prozesse werden jedoch isoliert betrachtet und die Schnittstellen sind nicht definiert. IT-Servicemanagement ist jedoch noch nicht als Managementaufgabe verankert und es gibt noch keine definierten Services.
- Definitionsgemäß agieren IT-Organisationen ab der **Stufe 4** prozessorientiert und zunehmend serviceorientiert. Bei einer prozessorientierten Vorgehensweise werden Aufgaben nicht mehr allein innerhalb einer Organisationseinheit verantwortet. Sie werden stattdessen organisationsübergreifend anhand von in Prozessen beschriebenen Tätigkeiten bearbeitet und über Rollendefinitionen den Ressourcen aus den Organisationsbereichen zugeordnet. Mit der Prozessorientierung eng verbunden ist die Ausrichtung auf die Kunden. Hierbei versteht sich die IT-Organisation als Service-Provider, der seinen Kunden vertraglich geregelte Dienstleistungen mit definierten SLAs (Services) anbietet. Die Prozesse dienen dabei der Erbringung der Services. Allerdings werden die IT-Services auf dieser Stufe noch separat betrachtet und sind nicht in einen übergeordneten Servicemanagement- und Lifecycle-Prozess eingebunden. Auch übergeordnete Servicestrategieprozesse zur Verwaltung der Services existieren noch nicht.
- Bei IT-Organisationen auf **Stufe 5** erfolgen alle Tätigkeiten im Rahmen definierter IT-Services, die wiederum einen eigenen Lebenszyklus gemäß dem ITIL® V3 Service Lifecycle durchlaufen.

An die IT-Dokumentation leiten sich aus den fünf Stufen entsprechende Anforderungen ab. Bild 3.4 zeigt, welche wesentlichen zusätzlichen Dokumentationsanforderungen ein Wechsel in die nächst höhere Stufe mit sich bringt. Dank dieses modularen Aufbaus ist es auch jederzeit möglich, zusätzliche Dokumentationsbereiche zu ergänzen. Einen strukturierten Überblick über die Merkmale und die daraus resultierenden Dokumentationsanforderungen der fünf Stufen zeigt Tabelle 3.1.

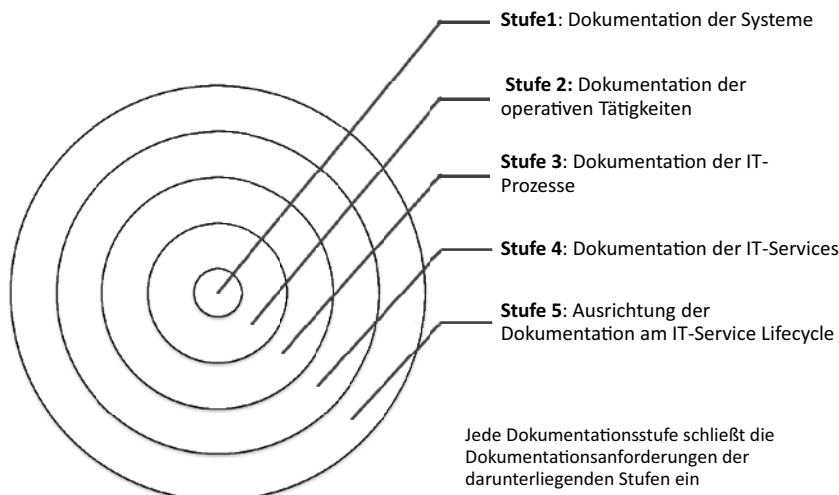


Bild 3.4 Hauptmerkmale der Betriebsdokumentation für die Stufen des Stufenmodells

- **Systemdokumentation:** Systeme bilden die Basis für die Bereitstellung von IT-Dienstleistungen, unabhängig davon, auf welcher Stufe sich eine IT-Organisation befindet. Die Einrichtung und Pflege einer Systemdokumentation (in Form von *Systemakten*) als Bestandteil der IT-Betriebsdokumentation sind daher für jede IT-Organisation zwingend erforderlich. Diese muss die eingesetzten Hardwarekomponenten (Server- und Clientsysteme) genauso beinhalten wie Beschreibungen des Verzeichnisdienstes, der Server- und Netzwerkdienste, der eingesetzten Software sowie der Netzwerkkomponenten. Zusätzlich gehören diverse Pläne wie beispielsweise Netzwerkkpläne zur Systemdokumentation.

Systemakten beschreiben (häufig automatisiert) die Komponenten eines Systems sowie deren Konfiguration und damit das technische „Was“. Hierzu zählen neben Systemspezifikationen auch Informationen zu Garantieleistungen, Wartungsverträge, Lizenzen und Ähnliches. Dies erfordert einen modularen Aufbau, was durch den Begriff Systemakte verdeutlicht wird. Ausführliche Erläuterungen zu den Systemakten finden Sie in *Kapitel 4*.

- **Dokumentation der operativen Tätigkeiten:** Diese Dokumentation soll vorrangig die Abläufe des täglichen operativen IT-Betriebs unterstützen. Sind die operativen Tätigkeiten gut und nachvollziehbar dokumentiert, erleichtern sie die täglichen Arbeitsabläufe. Außerdem können personelle Ausfälle leichter kompensiert werden und neue Mitarbeiter sich schneller einarbeiten. Da sich häufig Aufgabenbereiche definieren lassen, die sich auf mehrere Systeme beziehen, ist eine Trennung von den Systemakten sinnvoll. Meist werden die operativen Tätigkeiten in Form von Umsetzungskonzepten, Arbeitsanweisungen und Ablaufbeschreibungen dokumentiert. Die Dokumentation der operativen Tätigkeiten wird in *Kapitel 4, Abschnitt 4.3.4* vorgestellt.
- **IT-Prozessdokumentation:** Definierte, dokumentierte, wiederholbare und gelebte Prozesse sind die Basis einer erfolgreichen Serviceerbringung. Die Basis hierfür ist die Prozessdokumentation. Hierbei definiert die Prozessbeschreibung die Dokumentation eines einzelnen Prozesses (siehe *Abschnitt 3.4.4*). Die Prozessdokumentation umfasst als Gesamtheit die Beschreibungen aller Prozesse. Sie ist eine Managementaufgabe.
- **IT-Servicedokumentation:** Ein IT-Service ist eine in sich geschlossene Einheit, die dem Kunden angeboten wird, ohne ihn mit den einzelnen Systemkomponenten im Hintergrund, deren Zusammensetzung, Einzelkosten und Risiken zu konfrontieren. Intern besteht ein IT-Service in der Regel aus einer Vielzahl von IT-Komponenten (IT-Prozesse, Systeme, Ressourcen, Softwaresysteme, IT-Prozesse u. a.). Daraus leiten sich eine interne und eine externe Sicht auf die IT-Services ab, die sich auch in der Dokumentation widerspiegeln. Der Servicekatalog ist der nach außen hin sichtbare Teil. Er beinhaltet alle aktuell vereinbarten bzw. alle aktuell lieferbaren Services und gehört zu den wichtigsten Servicemanagement-Dokumenten (siehe *Abschnitt 3.4.2*).

Zusätzlich zu erstellen sind Dokumente zum Nachweis der Einhaltung gesetzlicher Anforderungen hinsichtlich Sicherheit und Datenschutz, die von allen IT-Organisationen unabhängig von der Stufe zu pflegen sind. *Kapitel 6* betrachtet ausführlich die Dokumentation für die drei Querschnittsthemen Informationssicherheit, Datenschutz und Notfallmanagement.

3.3.2.3 „Gebrauchsanweisung“ für die Nutzung des Stufenmodells

Für eine optimale Nutzung des Stufenmodells sollten Sie zuerst anhand der genannten Kriterien in der nachstehenden Tabelle 3.1 die für Ihre IT-Organisation passende Stufe ermitteln. Diese gibt einen strukturierten Überblick über die Merkmale und die daraus resultierenden Dokumentationsanforderungen der fünf Stufen.

In der Praxis ist natürlicherweise nicht immer eine eindeutige Zuordnung zu einer Stufe möglich. So kann es durchaus möglich sein, dass Ihre Organisation im operativen Bereich anlassbezogen arbeitet und nur wenige Verfahren dokumentiert sind, Sie für Ihre Kunden aber IT-Services anbieten und dafür auch bereits einen Servicekatalog erstellt haben. In diesem Fall müssen gegebenenfalls Bereiche aus mehreren Stufen kombiniert werden, was durch den modularen Aufbau des Stufenmodells ermöglicht wird.

Außerdem sind in der IT-Organisation möglicherweise der eine oder andere Service bei externen Dienstleistungsanbietern ausgelagert (beispielsweise das Webhosting, der Service Desk oder der Rechenzentrumsbetrieb). In diesem Fall können die Listen und Beschreibungen dazu verwendet werden, die Dokumentationsanforderungen an den jeweiligen Dienstleister zu identifizieren. Denn mit einer Auslagerung bzw. Outsourcing von Prozessen oder Verfahren ist kein Abwälzen der Geschäftsrisiken möglich. Die Risikoverantwortung obliegt auch bei Auslagerungen dem auslagernden Unternehmen. Sie müssen also bei Outsourcing sicherstellen bzw. sich davon überzeugen, dass die Compliance-Vorgaben, wie beispielsweise Sicherheits- und Datenschutzanforderungen, durch den Auftragnehmer erfüllt werden und nachweisbar dokumentiert sind.

Tabelle 3.1 zeigt in Abhängigkeit von der Ausprägung der drei Bereiche *IT-Services*, *IT-Prozesse* und *IT-System-/Infrastrukturbetrieb* für die fünf Stufen die spezifischen Anforderungen an die IT-Dokumentation.

Tabelle 3.1 Merkmale der Dokumentation für die fünf Stufen

IT-System-/ Infrastrukturbetrieb	IT-Prozesse	IT-Services	Umsetzung der Dokumentations- anforderungen
Stufe 1			
<ul style="list-style-type: none"> ▪ Operative Tätigkeiten zur Steuerung und zur Optimierung der Systeme erfolgen anlassbezogen und sind nicht standardisiert. ▪ Informationssicherheit ist auf IT-Sicherheit beschränkt und wird systembezogen betrachtet. 	<ul style="list-style-type: none"> ▪ Es gibt keine definierten Prozesse. 	<ul style="list-style-type: none"> ▪ Es gibt keine definierten IT-Services. 	<ul style="list-style-type: none"> ▪ Dokumentation der Systeme (Systembeschreibung, Betrieb und Administration sowie Systemsicherheit) in Systemakten ▪ IT-Sicherheitskonzept sowie Wiederherstellungspläne für kritische Systeme

Tabelle 3.1 Merkmale der Dokumentation für die fünf Stufen (*Fortsetzung*)

IT-System-/ Infrastrukturbetrieb	IT-Prozesse	IT-Services	Umsetzung der Dokumentations- anforderungen
Stufe 2			
<ul style="list-style-type: none"> ▪ Die operativen Tätigkeiten zur Steuerung und zur Optimierung der Systeme sind weitgehend standardisiert und durch Verfahren definiert. ▪ Informationssicherheit ist auf IT-Sicherheit beschränkt und wird systembezogen betrachtet. 	<ul style="list-style-type: none"> ▪ Es gibt keine definierten Prozesse. 	<ul style="list-style-type: none"> ▪ Es gibt keine definierten IT-Services. 	<ul style="list-style-type: none"> ▪ Dokumentation der Systeme (Systembeschreibung, Betrieb und Administration sowie Systemsicherheit) in Systemakten ▪ Umsetzungskonzepte, Ablaufbeschreibungen und Arbeitsanleitungen (einschließlich Aufzeichnungen) für die operativen Tätigkeiten ▪ IT-Sicherheitskonzept sowie Wiederherstellungspläne für kritische Systeme
Stufe 3			
<ul style="list-style-type: none"> ▪ Die operativen Tätigkeiten zur Steuerung und zur Optimierung der Systeme sind weitgehend standardisiert und durch Verfahren definiert. 	<ul style="list-style-type: none"> ▪ Einzelne Prozesse und IT-Service-management-Prozesse sind eingerichtet (z. B. für das Störungsmanagement). ▪ Prozesse werden isoliert betrachtet, Schnittstellen sind nicht definiert. ▪ IT-Sicherheit ist Bestandteil eines übergeordneten ISMS-Prozesses. 	<ul style="list-style-type: none"> ▪ Es gibt keine oder gegebenenfalls einzelne IT-Services. ▪ IT-Service-management ist noch nicht als Managementaufgabe implementiert. 	<ul style="list-style-type: none"> ▪ Dokumentation der Systeme (Systembeschreibung, Betrieb und Administration sowie Systemsicherheit) in Systemakten ▪ Umsetzungskonzepte, Ablaufbeschreibungen und Arbeitsanleitungen (einschließlich Aufzeichnungen) für die operativen Tätigkeiten ▪ IT-Sicherheitskonzept sowie Wiederherstellungspläne für kritische Systeme ▪ Dokumentation der Prozesse (Prozessbeschreibungen)

(Fortsetzung nächste Seite)

Tabelle 3.1 Merkmale der Dokumentation für die fünf Stufen (Fortsetzung)

IT-System-/ Infrastrukturbetrieb	IT-Prozesse	IT-Services	Umsetzung der Dokumentations- anforderungen
Stufe 4			
<ul style="list-style-type: none"> ▪ Wie bereits bei Stufe 3 ▪ Die operativen Tätigkeiten zur Steuerung und zur Optimierung der Systeme sind vollständig standardisiert und durch Verfahren definiert. 	<ul style="list-style-type: none"> ▪ Erforderliche Prozesse sind eingeführt und werden gesteuert. ▪ IT-Service-management-Prozesse dienen der Erbringung der definierten IT-Services. ▪ IT-Sicherheit ist Bestandteil eines übergeordneten ISMS-Prozesses. 	<ul style="list-style-type: none"> ▪ IT-Service-management ist als Managementaufgabe implementiert. ▪ IT-Services werden in einem IT-Servicekatalog gepflegt. 	<ul style="list-style-type: none"> ▪ Dokumentation der Systeme (Systembeschreibung, Betrieb und Administration sowie Systemsicherheit) in Systemakten ▪ Umsetzungskonzepte, Ablaufbeschreibungen und Arbeitsanleitungen (einschließlich Aufzeichnungen) für die operativen Tätigkeiten ▪ IT-Sicherheitskonzept sowie Wiederherstellungspläne für kritische Systeme ▪ Dokumentation der Prozesse (Prozessbeschreibungen) ▪ Servicebeschreibungen und Ergebnisdokumente der Serviceerbringung
Stufe 5			
<ul style="list-style-type: none"> ▪ Die operativen Tätigkeiten erfolgen im Rahmen definierter IT-Services. 	<ul style="list-style-type: none"> ▪ Prozesse werden im Rahmen des IT-Service-managements verwaltet. 	<ul style="list-style-type: none"> ▪ IT-Service-management ist eingeführt und IT-Services werden im Rahmen ihres Lifecycle gesteuert. 	<ul style="list-style-type: none"> ▪ Dokumentation der Systeme (Systembeschreibung, Betrieb und Administration sowie Systemsicherheit) in Systemakten ▪ Sicherheits- und Notfalldokumentation als Bestandteil des Information Security Managements und des IT-Service Continuity Managements ▪ Dokumentation der Prozesse (Prozessbeschreibungen) ▪ Servicebeschreibungen und Ergebnisdokumente der Serviceerbringung

Exemplarisch zeigen Bild 3.5 und Bild 3.6 die mögliche Strukturierung der IT-Service-managementdokumentation für die beiden Stufen vier und fünf. Während es bereits auf Stufe drei vereinzelte IT-Service-Prozesse gibt, stehen auf Stufe vier die Homogenität und Schnittstellen bzw. Querbeziehungen der ITSM-Prozesse und -Services untereinander im Fokus. Hierzu ist die Einrichtung steuernder IT-Service-management-Prozesse einschließlich entsprechender Vorgabedokumente erforderlich.

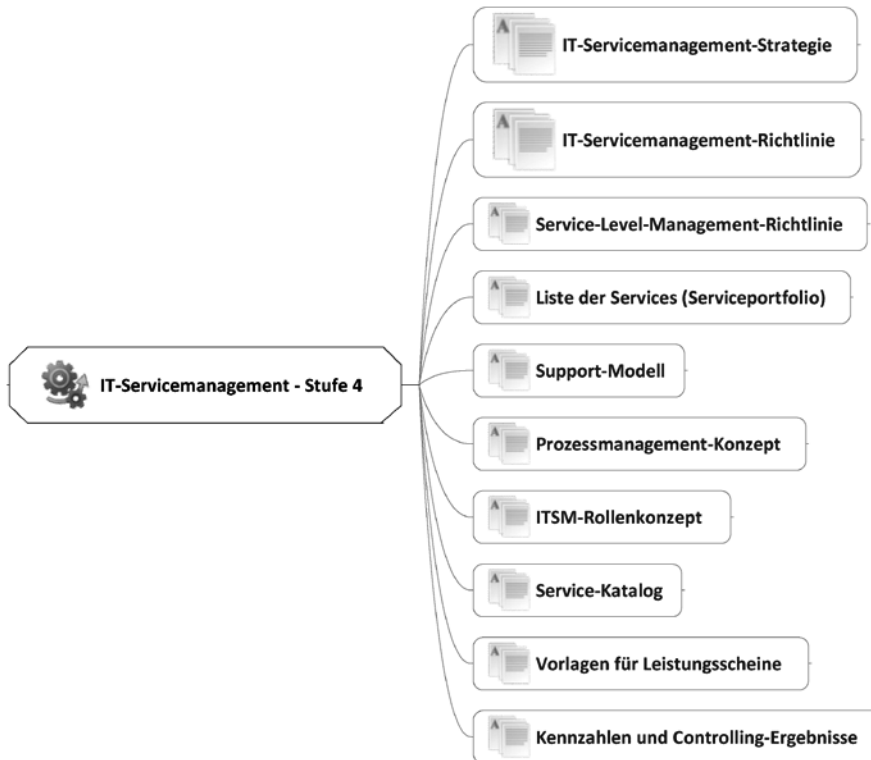


Bild 3.5 Exemplarischer Inhalt der IT-Service-managementdokumentation auf Stufe 4

Die Abbildung der Dokumentation im Bereich IT-Service-management für die Stufe fünf basiert auf der *IT Infrastructure Library (ITIL®)*. Mit Erreichen der fünften Stufe werden definitionsgemäß die Bedingungen zur Festlegung und Überwachung von Service Levels geschaffen. Hierfür ist u. a. ein Service-Level-Management-Prozess erforderlich, aber auch Capacity-, Availability- und IT Service Continuity Management, um sicherzustellen, dass die relevanten Service-Level-Ziele jederzeit erreicht werden. Die *Servicestrategie* bildet den Ausgangspunkt für alle Aktivitäten des Service Lifecycle. Sie beinhaltet die Ausrichtung des IT Service Management und stellt dessen Orientierung am Bedarf des Business sicher. Wichtige Themenfelder der Strategie sind Strategy Management, Business Relationship Management, Financial Management, Service Portfolio Management und Demand Management. Das *Service Design* setzt die Vorgaben aus der Strategie um und liefert entsprechende Vorlagen für die IT-Service-management-Prozesse bzw. IT Services.

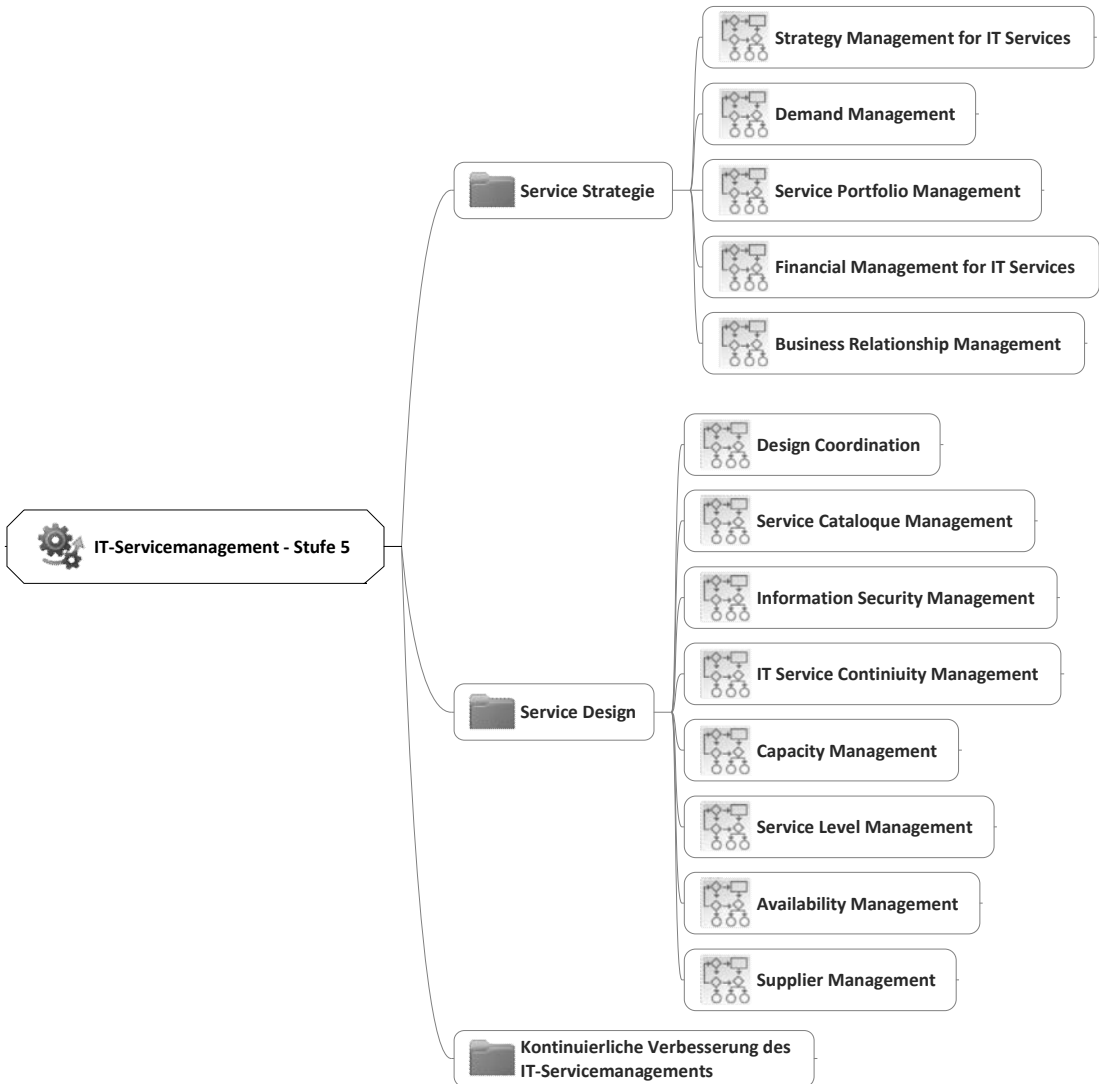


Bild 3.6 Exemplarische Inhalte der IT-Servicemanagementdokumentation auf Stufe 5 (Strukturierung der Prozesse für Service Design und Service Strategie gemäß ITIL®)

Eine besondere Bedeutung kommt auf Stufe 5 dem Prozess zur regelmäßigen Verbesserung des IT-Servicemanagements und damit auch seiner Dokumentation zu. Wichtig ist es darzulegen, dass Service Management nicht nur auf dem Papier existiert, sondern in allen Prozessen auch tatsächlich gelebt wird. Dieser Nachweis muss ganzheitlich erbracht werden. Es liegt in der Verantwortung des Managements, dass die Grundsätze und sämtliche Prozesse:

- dokumentiert,
- kommuniziert,

- gelebt,
- regelmäßig überprüft und
- verbessert werden.

Dazu braucht es Vorgabedokumente und entsprechende Aufzeichnungen.



Stufenmodell ist keine Umsetzung vorhandener Reifegradmodelle

Bei den im Buch definierten Stufen handelt es sich um einen Ansatz zur Strukturierung der IT-Betriebsdokumentation auf Basis praktischer Erfahrungen und in Anlehnung an vorhandene Reifegradmodelle. Es handelt sich nicht um ein Vorgehensmodell zu deren Umsetzung (beispielsweise nach ITIL® oder CMMI).

■ 3.4 Wichtige Dokumente des IT-Service-managements

Ein *IT-Service* ist eine in sich geschlossene Einheit (ein Produkt), die dem Kunden angeboten wird, ohne ihn mit den einzelnen Service-Komponenten, deren Zusammensetzung, Einzelkosten und Risiken zu konfrontieren. Die Mitarbeiter der IT-Organisation, die für die Bereitstellung der Services verantwortlich sind, haben zwangsläufig eine andere Sicht auf die IT-Services. Sie benötigen Informationen zu Beziehungen und technischen Komponenten.

Daraus leiten sich eine interne und eine externe Sicht auf die IT-Services ab, die sich auch in der Dokumentation widerspiegeln.

3.4.1 Servicebeschreibungen (SLAs)

In der Regel wird mit der Dokumentation der internen Sicht in Form von Servicebeschreibungen begonnen. Zusätzlich werden meist auch die Bedingungen zur Festlegung und Überwachung von Service Level geschaffen. Ziel des Service Level Management sind die Definition, Vereinbarung und das Management von Servicevereinbarungen, sogenannte *Service Level Agreements* - *SLAs*. Ein SLA - auch als Dienstgütereinbarung oder Dienstleistungsvereinbarung bezeichnet - ist eine Vereinbarung zwischen einem Auftraggeber und einem Dienstleister für wiederkehrende Dienstleistungen bzw. hier von IT-Services. Ziel ist es, die Kontrollmöglichkeiten für den Auftraggeber transparent zu machen, indem zugesicherte Eigenschaften wie Leistungsumfang, Reaktionszeit und Dienstgüte (Service Level) beschrieben werden. Werden IT-Services innerhalb eines Unternehmens anderen Organisationen bereitgestellt, wird hingegen der Begriff *Operation Level Agreement* - *OLA* verwendet. Im Gegensatz zu einer SLA ist ein Operating Level Agreement eine interne Leistungsvereinbarung zwischen Leistungserbringern innerhalb der IT-Organisation, die es

ermöglicht, Vereinbarungen aus SLAs umzusetzen. In der Praxis werden die konkreten Vereinbarungen zwischen Auftraggeber und Dienstleister häufig in Form von *Leistungsscheinen* vereinbart.

Gemäß BEIMS [2012] sollten die folgenden Attribute in einer Servicebeschreibung enthalten sein:

- *„Servicename und -beschreibung: Stellen die eindeutige Identifizierung des Service sicher und beschreiben, was dieser Service leistet.*
- *Status: Beschreibt, in welchem Status sich der Service in der Organisation befindet. Mögliche Status sind ‚definiert‘, ‚genehmigt‘, ‚entwickelt‘, ‚in Betrieb‘.*
- *Klassifizierung: Welche Bedeutung hat dieser Service für das Business?*
- *Genutzte Applikationen und Daten: Welche Anwendungen, Systeme und Daten werden für den Service benötigt?*
- *Unterstützter Geschäftsprozess: Zu welchem Geschäftsprozess leistet dieser Service welchen Beitrag?*
- *Business Owner, Business User, IT-Owner: Wer ist für den Service verantwortlich?*
- *Zugesicherte Eigenschaften (SLA): Welche Eigenschaften wie z. B. Verfügbarkeit oder Performance werden dem Kunden zugesichert?*
- *Unterstützende Services und Ressourcen: Welche Ressourcen und welche anderen Services werden benötigt, um diesen Service zu liefern?*
- *OLA, Contracts: Welche Vereinbarungen wurden intern und extern für die Serviceerbringung getroffen?*
- *Servicekosten und Servicepreis: Zu welchem Preis wird der Service erbracht und welche Kosten entstehen dadurch? (Die Kosten werden bei einem externen Provider in der Regel nicht transparent für den Kunden, es besteht allerdings diese Möglichkeit durch Open-Book-Kalkulation.)*
- *Metriken: Welche Messgrößen werden erfasst, wie werden sie erfasst und wie sieht der Report aus?“ [Beims 2012]*

3.4.2 Servicekatalog

Die Erstellung eines Servicekatalogs ist dann konsequenterweise der nächste Schritt. Deswegen originäre Aufgabe ist es, die Kunden über die angebotenen Produkte zu informieren, und er repräsentiert damit die externe Sicht. Zusätzlich werden häufig aber auch die intern erforderlichen Informationen im Servicekatalog beschrieben. Er gehört damit zu den wichtigsten Dokumenten eines an den Services ausgerichteten IT-Betriebs und enthält ausschließlich die aktiven und genehmigten Services inklusive aller notwendigen Informationen. Dazu gehört neben einer detaillierten Beschreibung der jeweiligen IT-Leistungen u. a. auch die Verfügbarkeit der Services.

Der IT-Servicekatalog stellt das Leistungsverzeichnis der IT-Organisation dar. Er beschreibt gemäß ITIL® in einer Datenbank oder einem Dokument alle IT-Services, die ein Unternehmen seinen Mitarbeitern oder Kunden anbietet. Er kann sowohl je Kunde als auch als Gesamtkatalog für alle Kunden definiert sein. Der Servicekatalog enthält ausschließlich die

aktiven und genehmigten Services inklusive aller notwendigen Informationen. Dazu gehören neben einer detaillierten Beschreibung der jeweiligen IT-Leistungen u. a. Verfügbarkeit der Services sowie die gegenseitigen Abhängigkeiten der Services. Weiterhin enthält der Servicekatalog in vielen Fällen auch die Preise und die SLAs (Service Level Agreements). Es ist jedoch auch möglich bzw. üblich, die SLA-Vereinbarungen in gesonderten Dokumenten, wie den im vorstehenden Abschnitt beschriebenen Servicebeschreibungen, zu verwalten.

Gemäß ITIL® kann im Servicekatalog neben der externen Sicht (die Business-Perspektive) auch die interne Sicht (die technische Perspektive) auf die IT-Services abgebildet werden. Er wird daher häufig strukturiert in einen *Business-Servicekatalog* und einen *Technischen Servicekatalog*.

Die Business-Perspektive beschreibt die Services aus Sicht des Kunden und enthält die Details aller IT-Services, die den Kunden bereitgestellt werden. Sie stellt außerdem die Beziehungen zwischen den IT-Services und den davon abhängigen Geschäftsbereichen und Businessprozessen dar. Der Business-Servicekatalog ist für den Kunden sichtbar.

Der technische Servicekatalog enthält Details zu allen IT-Services sowie die Beziehungen zu den unterstützenden Services, Applikationen, Serviceprozessen und technischen Komponenten, die notwendig sind, um den IT-Service für das Business bereitzustellen. Dieser Teil des Servicekatalogs ist nur für Mitarbeiter der IT-Abteilung sichtbar.

Für jeden Service sollte der Servicekatalog gemäß ITIL® die folgenden Informationen enthalten. Welche Inhalte der externen und welche der internen Sicht zuzuordnen sind, ist dann individuell festzulegen.

- Servicenamen,
- Servicebeschreibung,
- Servicetyp,
- unterstützende Services,
- Business Owner,
- Geschäftsbereiche,
- Business-Auswirkungen,
- Business-Priorität,
- Service Owner,
- Service Level Agreement,
- Service-Level-Klassen,
- Sicherheitsstufe/-klasse,
- Servicezeiten,
- Business-Kontakte,
- Eskalationskontakte,
- Serviceberichte,
- Service Reviews. [ITIL 2011]



Aufbau der Dokumentation ist auch abhängig von eingesetzten Fachanwendungen

IT-Servicemanagement ohne die Unterstützung entsprechender Tools ist nur schwer darstellbar. So ist der Betrieb eines Service Desk ohne ein Ticketsystem wohl nur in Ausnahmefällen möglich. Klassische Tools für das ITSM sind u. a.:

- Tickettools für das Incident-, Change- und/oder Problemmanagement,
- CMDB-(Configuration Management Database-)Tools zur Speicherung von Konfigurationsdaten.

Zwar sind derartige Fachanwendungen keine Dokumentationslösungen, denn der originäre Einsatzzweck dieser Anwendungen ist nicht die Dokumentation, sondern die Unterstützung bei der operativen Serviceerbringung, dennoch spielen sie für die IT-Dokumentation eine wichtige Rolle. Ausführliche Erläuterungen dazu finden Sie in *Kapitel 7, Abschnitt 7.6*.

3.4.3 Leistungsscheine

SLAs sind Vereinbarungen zwischen einem Service Provider und Auftraggeber bezüglich der Servicequalität und -quantität sowie der Ziele für die Serviceerbringung. Sie bilden die Basis für die Beziehung zwischen Service Provider und Kunden. Anhand dieser verbindlichen Vereinbarung können Kunden und deren Mitarbeiter erkennen, welche Services zu erwarten sind, und der Service Provider hat eine eindeutige Grundlage für die Gestaltung und Lieferung der Services. In der Praxis werden die konkreten Vereinbarungen zwischen Auftraggebern und Dienstleister häufig in Form von *Leistungsscheinen* vereinbart.

Beispiel Leistungsschein

Tabelle 3.2 Exemplarischer Aufbau eines Leistungsscheins

Dienstleistungsbeschreibung	
Name des Service	<i>Name gemäß Servicekatalog</i>
Leistungsbeschreibung	<i>Falls vorhanden, auch Angaben zu den verarbeitenden Mengen, z. B. Bandbreitenangaben; außerdem Art des Service sowie die Verantwortlichkeiten</i>
Betriebs- und Servicezeiten	
Betriebszeiten	<i>Zeiträume, in welchen der Service nutzbar ist</i>
Servicezeiten	<i>Beispielsweise Wartungsfenster mit der entsprechenden Zeitperiode sowie einer Beschreibung</i>
Verfügbarkeit und Performance	
Verfügbarkeit	<i>Art, maximale Ausfalldauer sowie die maximale Anzahl der Ausfälle pro Zeitperiode</i>
Performanz	<i>Performanzparameter, z. B. Rückruf innerhalb von drei Stunden</i>
Technische Anforderungen	<i>Beschreibung der minimalen technischen Anforderungen</i>

Tabelle 3.2 Exemplarischer Aufbau eines Leistungsscheins (*Fortsetzung*)

Eskalation	
Kriterien und Reaktionszeit	<i>Eskalationsszenarien mit den vorgesehenen Reaktionszeiten</i>
Kritikalität	<i>Kritikalität gegebenenfalls pro Dienstleistung</i>
Sicherheitsanforderungen & Notfallvorsorge	
Sicherheitsanforderungen	<i>Art der Anforderungen mit einer kurzen Beschreibung und gegebenenfalls zugrunde liegende Compliance-Anforderungen (z. B. gesetzliche Anforderungen)</i>
Notfallvorsorge	<i>Definierte Notfälle und Maßnahmen sowie Verantwortlichkeiten (müssen jeweils mit dem Notfallvorsorgekonzept des Leistungsnehmers übereinstimmen)</i>
Risk Management	<i>Identifizierte Risiken</i>
Kosten	
Kosten	<i>Kosten, sofern verrechnet (gegebenenfalls Verweis auf weitere Dokumente)</i>

Außerdem erforderlich sind Beschreibungen aller Service-Management-Prozesse und Funktionen. Definierte, dokumentierte, wiederholbare und gelebte Prozesse sind die Basis einer erfolgreichen Serviceerbringung. Die Grundlage hierfür ist die Prozessdokumentation. Die Prozessdokumentation setzt sich zusammen aus den Prozessbeschreibungen der Einzelprozesse. Wie eine anforderungsgerechte Prozessdokumentation erstellt werden kann, ist Gegenstand des folgenden Abschnitts.

3.4.4 Prozessbeschreibungen

Gemäß der Definition des Bundesverwaltungsamts ist Prozessmanagement ein ganzheitliches, auf Dauer ausgerichtetes Vorgehen zur systematischen Identifikation, Dokumentation, Analyse, Optimierung, Steuerung, Überwachung und Weiterentwicklung von Prozessen [Bundesverwaltungsamt 2013].

An Prozessbeschreibungen sind die allgemeinen revisorischen Anforderungen zu stellen. Dementsprechend müssen sie für einen sachverständigen Dritten in angemessener Zeit nachvollziehbar, vollständig und aktuell sein. Vorgaben, in welcher Form Prozesse zu beschreiben sind, gibt es hingegen nicht. Die Dokumentation kann in jeder Form und Art und mit jedem beliebigen Medium erfolgen. Wichtig ist, dass alle Mitarbeiter Kenntnis von den Prozessen erhalten. Dazu müssen ihnen die Dokumente entweder an zentraler Stelle in Papierform vorliegen oder sinnvollerweise im Intranet einsehbar sein. Besonders hilfreich ist es, wenn die Prozessbeschreibungen mit Workflows verknüpft sind bzw. Links zu den relevanten Dokumenten enthalten, so dass die Benutzer direkt die für sie relevanten Dokumente öffnen können.

Es sollte darüber hinaus Verfahren geben, die die Erstellung, Freigabe, Bereitstellung und Änderung von Prozessdokumenten regeln. Die DIN-Norm 9001:2015 beispielsweise fordert explizit ein *Verfahren zur Lenkung dokumentierter Informationen*. Dieses muss die folgenden Aspekte regeln:

„a) Verteilung, Zugriff, Auffindung und Verwendung;

b) Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;

c) Überwachung von Änderungen (z. B. Versionskontrolle);

d) Aufbewahrung und Verfügung über den weiteren Verbleib

[...] Dokumentierte Informationen, die als Nachweis aufbewahrt werden, müssen vor unbeabsichtigten Änderungen geschützt werden.“ [ISO 9001:2015, 7.5.3]



Dokumentierte Informationen

Der Begriff der „Dokumentierten Informationen“ wurde von der International Organization for Standardization 2012 mit den ISO-IEC Directives Part 1 zur Entwicklung von ISO-Normen eingeführt. Sie sind definiert als die aus Sicht der jeweiligen Managementnorm vom Unternehmen zu lenkenden und nachzuweisenden (aufrechtzuerhaltenden) Informationen einschließlich der eingesetzten Medien. [ISO_IEC Directives Part 1 2014]

3.4.4.1 Inhalte einer Prozessbeschreibung

Eine Prozessbeschreibung enthält alle für einen Prozess relevanten Informationen. Die Dokumentation und Visualisierung von Prozessen bilden die Grundlage für Prozessoptimierungen und dienen als Nachweis der Einhaltung von Organisationspflichten.

Prozessbeschreibungen müssen so aufgebaut sein, dass sie alle wesentlichen Aspekte des Prozesses darstellen und eine Bewertung ermöglichen. Bei einem Audit werden für die Bewertung der zu prüfenden Prozesse die nachstehenden Kriterien zugrunde gelegt. Hier wird insbesondere darauf geachtet, dass die Prozesse eindeutig, lückenlos und konsistent beschrieben sind. Die Prozessbeschreibung sollte deshalb die folgenden Inhalte darstellen.

- **Prozessziele:** Die Prozesse wurden auf der Grundlage von Zielsetzungen entwickelt und umgesetzt. Die Prozessbeschreibung der Einzelprozesse muss demzufolge das Prozessziel und die daraus abzuleitenden Zielsetzungen messbar beschreiben.
- **Orientierung an Unternehmenszielen:** Die Zielsetzungen der einzelnen Prozesse stehen in Einklang mit den Unternehmenszielen und sind an diesen ausgerichtet.
- **Prozesswirksamkeit:** Die Wirksamkeit der Prozesse ist sicherzustellen. Dazu wird die Qualität der Prozesse regelmäßig anhand von Kennzahlen (KPI) überprüft und gegebenenfalls angepasst. Die Dokumentation der Prozesse wird gepflegt und ist mit den realisierten Prozessen konsistent, das heißt, die Prozesse werden tatsächlich in der dokumentierten Form angewendet.
- **Prozessverantwortlichkeiten:** Den Prozessen und jedem Prozessschritt sind eindeutige Verantwortlichkeiten zugeordnet.
- **Qualitätssicherung:** Die Prozesse beinhalten Prozessschritte, die die Qualität der erreichten (Zwischen-)Ergebnisse sicherstellen und die Ergebnisse dokumentieren.
- **Risiken:** Die Risiken und Gefahren, die mit einem Prozess verbunden sind, sind analysiert und beschrieben.

Die Schwierigkeit bei der Erstellung der Prozessdokumentation besteht in der Frage der Detaillierungstiefe. Soll diese nicht nur als Nachweis gegenüber der Unternehmensleitung und gegebenenfalls einem Prüfer dienen, sondern auch ein Arbeitsmittel für die Mitarbeiter darstellen, sind zusätzliche detaillierte Beschreibungen der Arbeitsabläufe sowie Checklisten und Formulare als Anlage zu den Prozessbeschreibungen unverzichtbar. Hierfür ist ein modularer Aufbau erforderlich.

Im Idealfall sind Prozessbeschreibungen so aufgebaut, dass sich einerseits die Unternehmensleitung einen schnellen Überblick verschaffen kann und andererseits der Anwender in der Lage ist, die ihm zugeordneten Tätigkeiten in der festgelegten Art und Weise zu erledigen. Mit der nachstehenden Struktur ist das gewährleistet. Dabei wird jede Prozessbeschreibung als eine Akte behandelt, die alle für den beschriebenen Prozess erforderlichen Dokumente enthält. Hierbei ist es wichtig, sich frühzeitig zu überlegen, wie und wo die Prozessdokumente veröffentlicht werden sollen (als Printversion oder im Intranet zum Beispiel).

Möglicher Aufbau einer Prozessbeschreibung:

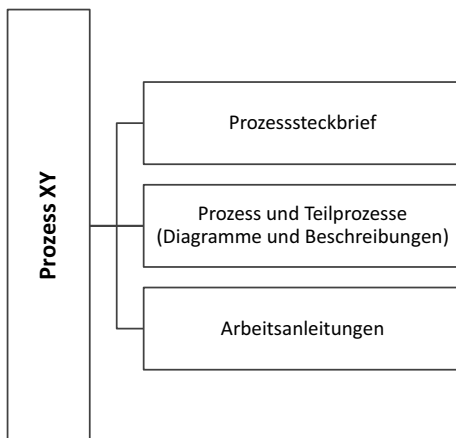


Bild 3.7

Mögliche Gliederung einer Prozessbeschreibung

3.4.4.2 Prozesssteckbrief

Jede Prozessbeschreibung sollte sinnvollerweise einen Prozesssteckbrief beinhalten. Der Prozesssteckbrief liefert einen schnellen Überblick über alle wichtigen Prozessmerkmale. Hierzu sind folgende Informationen erforderlich:

- **Prozessname:** Jeder Prozess erhält einen Namen, der möglichst eindeutig und prägnant das Ziel des Prozesses erkennen lässt. Möglich ist beispielsweise, festzulegen, dass der Prozessname immer aus einem Substantiv und einem Verb bestehen muss (zum Beispiel „Benutzerkonto einrichten“).
- **Prozessnummer:** Jeder Prozess benötigt eine eindeutige Nummer. Diese ermöglicht es beispielsweise, in unterschiedlichen Dokumenten auf den Prozess zu verweisen. Pfllegt das Unternehmen eine unternehmensweit durchgängige Prozessnummerierung (entweder in tabellarischer Form oder in einer *Prozesslandkarte*, so ist diese natürlich zu berücksichtigen. In diesem Fall enthält jeder IT-Prozess eine entsprechende übergeordnete Nummer vorangestellt, die die Einordnung in den Unternehmensprozesskontext ermöglicht. Alternativ ist eine gesonderte Nummerierung der IT-Prozesse möglich.

- **Beschreibung:** Die Beschreibung soll in aller Kürze die Aufgabe und das Ergebnis des Prozesses beschreiben.
- **Prozessziel:** Jeder Prozess muss zwingend ein definiertes Ziel haben. Dieses muss überprüfbar und eindeutig sein. Das Ziel muss außerdem durch den Prozess erreichbar sein. Ein Prozess darf also keine Parameter oder Ereignisse definieren, die nicht der Kontrolle des Prozesses unterliegen.
- **Prozessverantwortlicher:** Für jeden Prozess muss es einen Verantwortlichen geben. Dieser ist als Rolle und gegebenenfalls mit der Funktion in der Aufbauorganisation zu benennen.
- **Prozessteam:** Für alle Prozessschritte muss die Rolle benannt werden, die die jeweilige Aktivität zu erledigen hat. Dies kann in der grafischen Darstellung des Prozesses erfolgen oder in dessen detaillierter Beschreibung. Im Projektsteckbrief dagegen genügt es, die beteiligten Rollen aufzuführen.
- **Prozessauslösendes Ereignis:** Es muss eindeutig beschrieben sein, durch welches Ereignis der Prozess ausgelöst wird. So löst beispielsweise der Eingang einer E-Mail beim Service Desk einen Störungsprozess aus.
- **Prozessinput (Daten/Dokumente):** Es sollten die Inputkomponenten benannt werden, die den Prozess auslösen. Hierbei kann es sich sowohl um Dokumente handeln wie beispielsweise ein Formular oder auch um Daten, die das Ergebnis eines anderen Prozesses sind.
- **Prozessoutput (Daten/Dokumente):** Im Prozesssteckbrief sollten die wichtigsten Prozessergebnisse, z. B. eine ausgefüllte Checkliste, genannt werden. Dies gilt insbesondere für Dokumente oder Daten, die einen Input für einen Folgeprozess darstellen.
- **Schnittstellen zu anderen Prozessen:** Hat ein Prozess Schnittstellen zu anderen Prozessen – und es wird kaum Prozesse geben, bei denen dies nicht der Fall ist –, sind diese im Projektsteckbrief zu benennen.
- **Risiken und Gefahren:** Unter diesem Punkt sind Einflüsse zu benennen, die den Prozessverlauf behindern können.
- **Prozesskennzahlen/Messgrößen:** Ein Prozess kann nur dann im Sinne des Qualitätsmanagements optimiert werden, wenn sein Ergebnis messbar ist. Zu jeder Zielformulierung gehören daher sinnvolle und messbare Kriterien, mit denen der Erfüllungsgrad des Ziels ermittelt werden kann.
- **Prozess freigegeben am und freigegeben durch:** Prozesse müssen, wiederum im Rahmen eines entsprechenden Prozesses, geprüft und freigegeben werden. Im Prozesssteckbrief sollte vermerkt werden, wann und durch wen der Prozess vor der Inbetriebnahme freigegeben wurde.
- **Prozessbewertung (Verantwortlicher und Termin):** Prozesse sollten turnusmäßig daraufhin überprüft werden, ob sie noch effizient sind und ob das gewünschte Ziel mit dem minimal erforderlichen Aufwand erzielt wird. Es ist sinnvoll, im Prozesssteckbrief einzutragen, wann die nächste Überprüfung erfolgen soll und durch wen.
- **Arbeitsanleitungen:** Sind dem Prozess andere Dokumente wie beispielsweise Formulare oder Checklisten zugeordnet, sollte im Prozesssteckbrief darauf verwiesen werden.

Das nachstehende Beispiel zeigt exemplarisch den Aufbau eines solchen Prozesssteckbriefs.

Tabelle 3.3 Muster – Prozesssteckbrief

Prozesssteckbrief			
Prozessname:		Prozess-Nr.	
Kurzbeschreibung:			
Prozessziel:			
Rollen			
Prozessverantwortlicher:		Prozessteam (Rollen):	
Prozessinput (Daten/Dokument)			
Prozessoutput (Daten/Dokumente)			
Prozessauslösendes Ereignis			
Schnittstellen zu anderen Prozessen			
Risiken und Gefahren			
Prozesskennzahlen Messgrößen			
Prozess freigegeben am		Freigegeben durch:	
Prozessbewertung durch		Termin/Turnus:	
Arbeitsanweisungen			

3.4.4.3 Grafische Prozessbeschreibungen

Prozesse können auf unterschiedliche Weise dokumentiert werden. Dies kann im einfachsten Fall sogar Fließtext oder eine Tabelle sein. In der Praxis werden Prozesse meist grafisch in Form eines Ablaufdiagramms dargestellt, das den Prozess veranschaulicht und dem eine textliche Beschreibung vorangestellt ist. Hierbei ist die grafische Darstellung der Prozesse als Ergänzung der Prozessbeschreibung zu betrachten. Sie kann in der Regel eine detaillierte Beschreibung der Abläufe nicht ersetzen.

Bevor also mit der Dokumentation von Prozessen begonnen werden kann, müssen das Prozessmodell und die Modellierungswerkzeuge ausgewählt werden. Zur Auswahl stehen eine Reihe von Techniken von einfachen Flussdiagrammen bis zu standardisierten Modellierungsmodellen, wie beispielsweise *Business Process Modeling Notation (BPMN)*, *Unified Modeling Language (UML)* und *Ereignisgesteuerte Prozessketten (EPKs)*.

Darüber hinaus sind weitere Modellierungsregeln zu definieren. Hierzu zählen zum Beispiel:

- Welche Symbole (Objekte) werden zur Prozessbeschreibung eingesetzt?
- In welcher Sprache wird modelliert?
- Welche und wie viele Beschreibungsebenen werden eingerichtet?

- Wie werden die Prozesse und Teilprozesse der verschiedenen Beschreibungsebenen bezeichnet?
- In welcher Art werden Schnittstellen zwischen den Teilprozessen dargestellt und wie werden diese bezeichnet?
- Welche Rollen gibt es (siehe Rollenkonzept in *Abschnitt 3.4.6*)?



Begriff Workflow

Auch im Bereich der Prozessmodellierung findet man viele unterschiedliche Begriffe, die mit gänzlich unterschiedlicher Bedeutung verwendet werden. Ein typisches Beispiel hierfür ist der Begriff *Workflow*, der in mannigfaltiger Weise benutzt wird.

Auf eine Verwendung des Begriffs *Workflow* wird an dieser Stelle verzichtet, da dieser Begriff mit so unterschiedlichen Bedeutungen besetzt ist, dass dies zu Verwirrungen führen würde.

Im Bereich der IT-Dokumentation gehören EPKs und Darstellungen als Flussdiagramme zu den am weitesten verbreiteten Darstellungsformen. Diese und zwei damit verwandte Typen werden im Folgenden näher vorgestellt.

Ereignisgesteuerte Prozesskette (EPK)

Ereignisgesteuerte Prozesskette (EPK) ist ein Modell zur Darstellung von Prozessen und ein wesentliches Element des ARIS-Konzepts der Firma IDS Scheer. Das Modell wurde 1992 von einer Arbeitsgruppe an der Universität des Saarlandes zusammen mit der SAP AG zur Dokumentation von Geschäftsprozessen entwickelt. ARIS (Architektur integrierter Informationssysteme) und die ereignisgesteuerten Prozessketten haben sich mittlerweile zu einem Quasistandard für die Geschäftsprozessmodellierung insbesondere bei SAP-gestützten Unternehmensprozessen entwickelt.

EPKs stellen einen Prozess als eine Kette von Tätigkeiten (im EPK-Modell als *Funktionen* bezeichnet) dar, die wiederum durch *Ereignisse* verknüpft sind. Eine Funktion hat als Eingang definierte Ereignisse, die eingetreten sein müssen, bevor die Funktion ausgeführt werden kann (Startereignisse). Eine Funktion, die ausgeführt wird, erzeugt wiederum ein oder mehrere Ereignisse. Jede Funktion kann zusätzlich mit einem Informationsobjekt verbunden werden. Diese dienen dazu, das Einspielen oder Speichern von Informationen darzustellen.

Durch eine zusätzliche Verknüpfung von Ereignissen durch logische Konnektoren können parallele Abläufe oder alternative Abläufe dargestellt werden:

- **AND – Und-Verknüpfung:** Die Aussage ist wahr, wenn beide Aussagen gleichzeitig wahr sind.
- **OR – Und-oder-Verknüpfung:** Die Aussage ist wahr, wenn mindestens eine Aussage gleichzeitig wahr ist.
- **XOR – Entweder-oder-Verknüpfung:** Die Aussage ist wahr, wenn genau eine der beiden Aussagen wahr ist.

Eine ereignisgesteuerte Prozesskette besteht demzufolge aus drei möglichen Knotentypen:

- **Funktion:** Funktionen bilden die Grundbausteine des Diagramms. Jede Funktion entspricht einer ausgeführten Aktivität.
- **Ereignis:** Ereignisse können vor und/oder nach der Ausführung einer Funktion auftreten und sind durch Ereignisse verbunden.
- **Konnektor:** Konnektoren verknüpfen Funktionen und Ereignisse. Es gibt drei Typen: UND, ODER sowie das ausschließende ODER (XOR).

Zusätzlich zu den genannten Grundelementen können EPKs um zusätzliche Elemente erweitert werden. Beim Verwenden dieser Elemente spricht man von *erweiterten EPKs (eEPK)*. So können beispielsweise die mit der Ausführung von Funktionen betrauten Organisationseinheiten sowie ein- und ausgehende Datenobjekte dargestellt werden. Somit ermöglichen erweiterte EPKs eine Prozessverfolgung über mehrere Organisationseinheiten hinweg. Bild 3.8 zeigt einen in EPK-Notation verfassten Prozess.

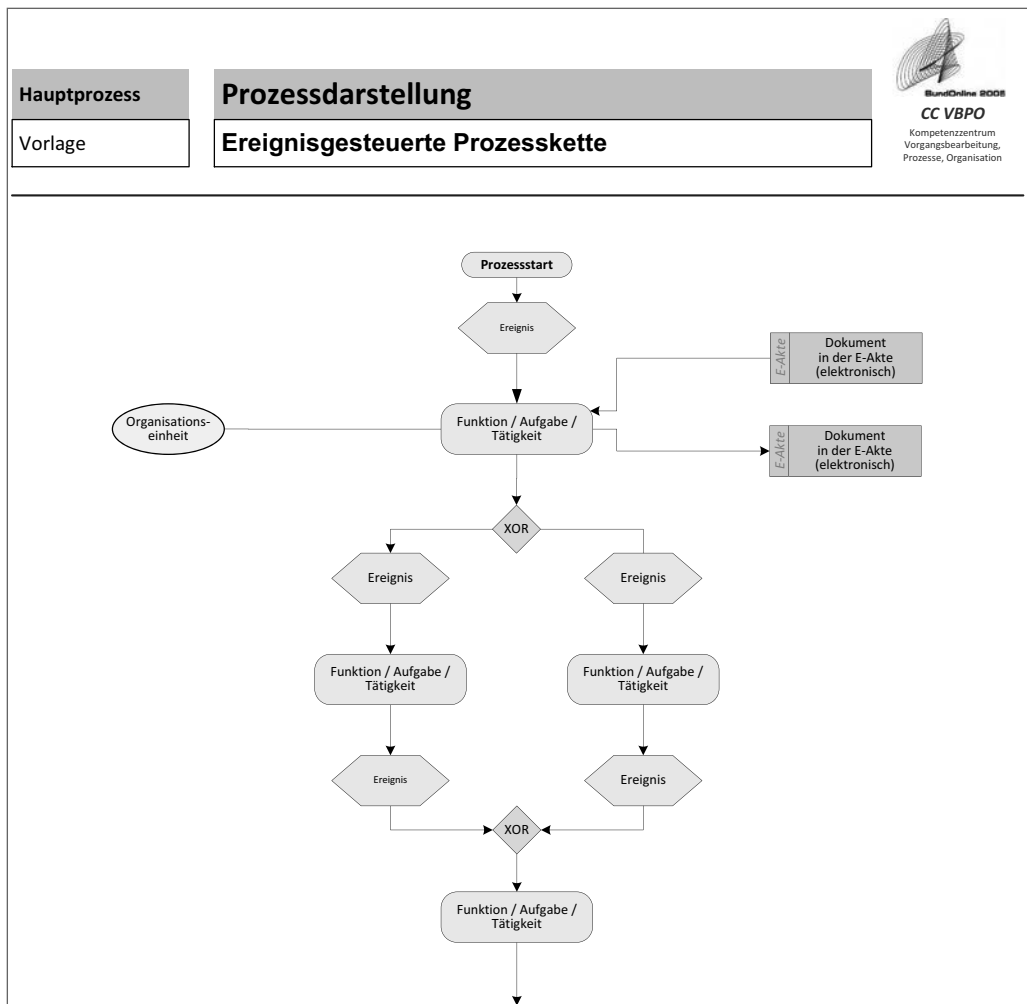


Bild 3.8 Beispiel EPK-Notation. Quelle: Bundesverwaltungsamt [2010]

EPKs sind gut geeignet für die Darstellung von Prozessen, können jedoch sehr lang werden, da für alle Funktionen dargestellt werden muss, durch welche Ereignisse sie initiiert werden. Die formale Form der EPKs bedingt auch, dass Verzweigungen und Schleifen schwer darstellbar sind, so dass sie für die detaillierte Darstellung von Arbeitsabläufen nicht gut geeignet sind.

Flussdiagramme

Flussdiagramme sind eine einfache und häufig eingesetzte Darstellungsform, um Prozesse und Arbeitsabläufe zu dokumentieren. Im Gegensatz zu EPKs unterliegen Flussdiagramme keinen Standardisierungsregeln. Zwar definiert die DIN 66001 von 1966 bzw. die ISO-Norm 5807 einen Satz von Symbolen (engl. Shapes) für Datenfluss- und Programmablaufpläne und dieser hat sich ebenfalls weitgehend als Symbolsatz zur Darstellung von Prozessen und Tätigkeiten durchgesetzt, verbindliche Regelungen für deren Verwendung, wie dies bei EPKs der Fall ist, gibt es aber nicht.

Weit verbreitet ist die Verwendung von in Flussdiagrammen (auch als Swimlanes – Schwimmbahnen bezeichnet). Mithilfe von Funktionsbändern kann die Beziehung zwischen einer Aktivität und dem für diese Aktivität verantwortlichen Bearbeiter bzw. der Organisationseinheit dargestellt werden. Hierzu werden die Tätigkeiten in den Bändern platziert, die den für diese Schritte verantwortlichen Funktionseinheiten entsprechen. Grundsätzlich können Funktionsbänder auch bei der Modellierung mit EPKs eingesetzt werden. Sie finden dort aber seltener Anwendung.

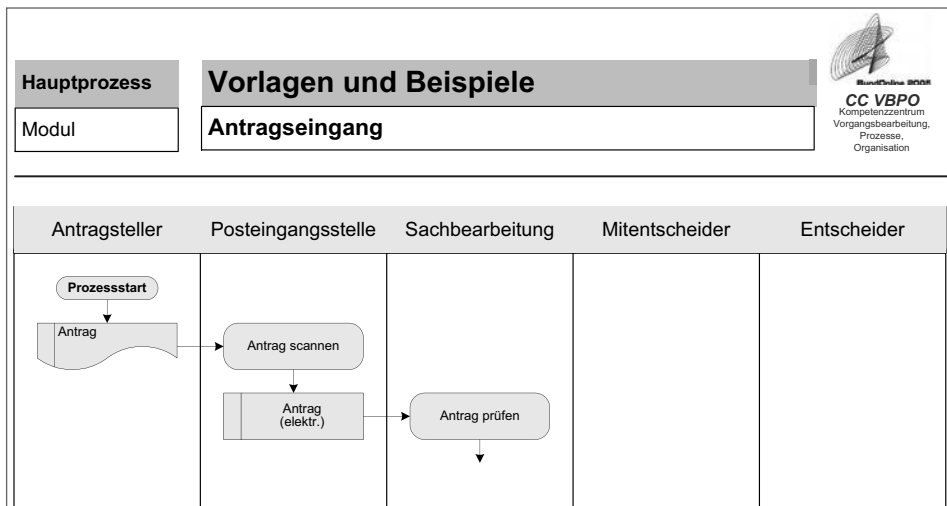






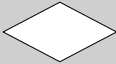



Bild 3.9 Beispiel Flussdiagrammnotation. Quelle: Bundesverwaltungsamt [2013]

Um die allgemeine Verständlichkeit und Einheitlichkeit der Prozessbeschreibungen zu gewährleisten, sollte eine standardisierte Beschreibungssprache in Form von Symbolen (Notation) eingesetzt werden. Die nachstehenden Symbole zum Beispiel werden häufig verwendet. In der Praxis finden bei Flussdiagrammdarstellungen vor allem die folgenden Symbole Anwendung:

Symbol	Bezeichnung	Symbol	Bezeichnung
	Start / Ende		Daten
	Prozess		Dokument
	Teilprozess		Externe Daten
	Entscheidung		Datenbank

Eine spezielle Form der Flussdiagrammdarstellung ergibt sich aus der Kombination von Flussdiagrammen und RACI bzw. RASCI-Modellen. *RACI-Diagramme* sind eine Technik zur Analyse und Darstellung von Verantwortlichkeiten, deren Name sich aus den Anfangsbuchstaben der englischen Begriffe *Responsible, Accountable, Supportive, Consulted* und *Informed* ableitet.

Diese Verantwortlichkeiten werden im Diagramm eingetragen. Sie tragen die folgenden Abkürzungen:

- **Responsible (R):** verantwortlich. Der Rolleninhaber ist für die Durchführung verantwortlich. Dies wird auch als sachliche Verantwortung bezeichnet.
- **Accountable (A):** rechenschaftspflichtig. Der Rolleninhaber muss „genehmigen und abzeichnen“ und ist im rechtlichen oder kaufmännischen Sinne für das Ergebnis und die Qualität verantwortlich. Dies wird auch als Verantwortung aus Kostenstellensicht bezeichnet.
- **Supportive (S):** unterstützend. Der Rolleninhaber hat eine unterstützende Funktion und kann Sachmittel zur Verfügung stellen.
- **Consulted (C):** beratend. Der Rolleninhaber hat eine beratende Funktion. Dies wird auch als Verantwortung aus fachlicher Sicht bezeichnet.
- **Informed (I):** informiert. Der Rolleninhaber erhält Informationen über den Verlauf bzw. das Ergebnis der Tätigkeit oder besitzt die Berechtigung, Auskunft zu erhalten.

RACI-Diagramme

RACI-Diagramme dienen zur Beschreibung, welche Rolle für welche Tätigkeiten verantwortlich ist und welche Rollen zu beteiligen sind. Für jeden Prozessschritt wird bei dieser Darstellung zusätzlich angegeben, welche Rolle verantwortlich ist, wer Richtlinienkompetenz besitzt und genehmigt, wer den Prozess beratend unterstützt und welche Rolle informiert wird. Im Vordergrund steht hierbei die Beschreibung der Verantwortlichkeiten und Zuständigkeiten.

Da bei dieser speziellen Form eines Flussdiagramms nicht der Prozessablauf, sondern die Darstellung der Verantwortlichkeiten im Vordergrund steht, ist der verfügbare Platz für das eigentliche Flussdiagramm zwangsläufig beschränkt. Insofern eignen sich RACI-Diagramme weniger für eine detaillierte Darstellung komplexer Arbeitsflüsse, als vielmehr zur

übersichtlichen Dokumentation von Prozessen und zu den damit zugeordneten Verantwortlichkeiten. Im Rahmen der Dokumentation zur Erlangung einer ISO-Zertifizierung stellen sie allerdings eine häufig verwendete Darstellungsform dar.

Bild 3.10 zeigt exemplarisch ein an die RACI-Notation angelehntes Flussdiagramm. Abweichend von RACI werden im Beispiel nur die Verantwortungen *Responsible*, *Supportive* und *Informed* dargestellt.

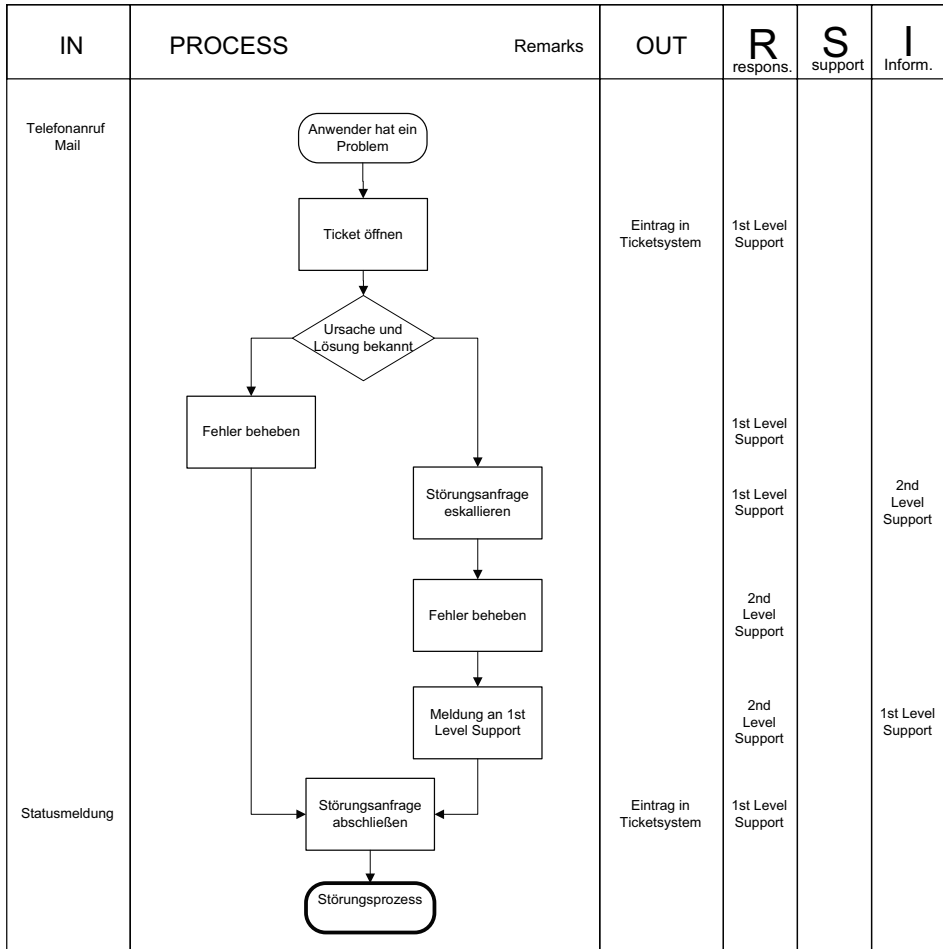


Bild 3.10 Beispielprozess in RSI-Notation

Kommunikationsstrukturanalyse (KSA)

Die KSA-Methode ist in den späten 1980er-Jahren an der Technischen Universität Berlin unter dem Namen *Kommunikationsstrukturanalyse (KSA)* entwickelt worden. KSA-Modelle zählen zur Gruppe der Informationsmodelle und dienen der hierarchischen Strukturierung der zu bearbeitenden Aufgaben und Informationen. Der Fokus von KSA-Modellen liegt also auf der Beschreibung, Analyse und Optimierung von Informationsflüssen. Betrachtet wird dabei der Austausch von Informationen und Informationsträgern zwischen den Prozess-

schritten und ihren Bearbeitern. Die Vorgehensweise dabei ist top-down. Ein Prozess im KSA-Modell ist eine Abfolge von Tätigkeiten (Aufgaben) mit definierten Schnittstellen wie Eingängen und Ausgängen. Zwischen diesen Prozesselementen gibt es Informationsflüsse (z. B. „Schickt Info“), bei denen angegeben werden kann, welche Informationen zwischen zwei Tätigkeiten sowie den Prozessschnittstellen fließen. Weitere Prozesselemente sind Sachmittel und Speicher, die mit den Tätigkeiten verbunden werden können. Alle Prozesselemente können wahlweise auch in Funktionsbändern angeordnet und so einem Bearbeiter zugeordnet werden.

KSA-Modelle werden bevorzugt im Qualitätsmanagement eingesetzt. Außerdem entsprechen sie den Standards der *Workflow Management Coalition (WfMC)*. Diese Organisation wurde 1993 gegründet und stellt einen Verbund von mehreren Hundert Herstellern, Nutzern, Beratern und Wissenschaftlern im Bereich des Workflow-Managements dar. Hauptziel der WfMC ist die Etablierung eines Workflow-Referenzmodells. Dieses spezifiziert die Struktur für Workflow-Management-Systeme sowie deren Charakteristika, Funktionen und Schnittstellen. Bild 3.11 zeigt exemplarisch einen Prozess in KSA-Notation:

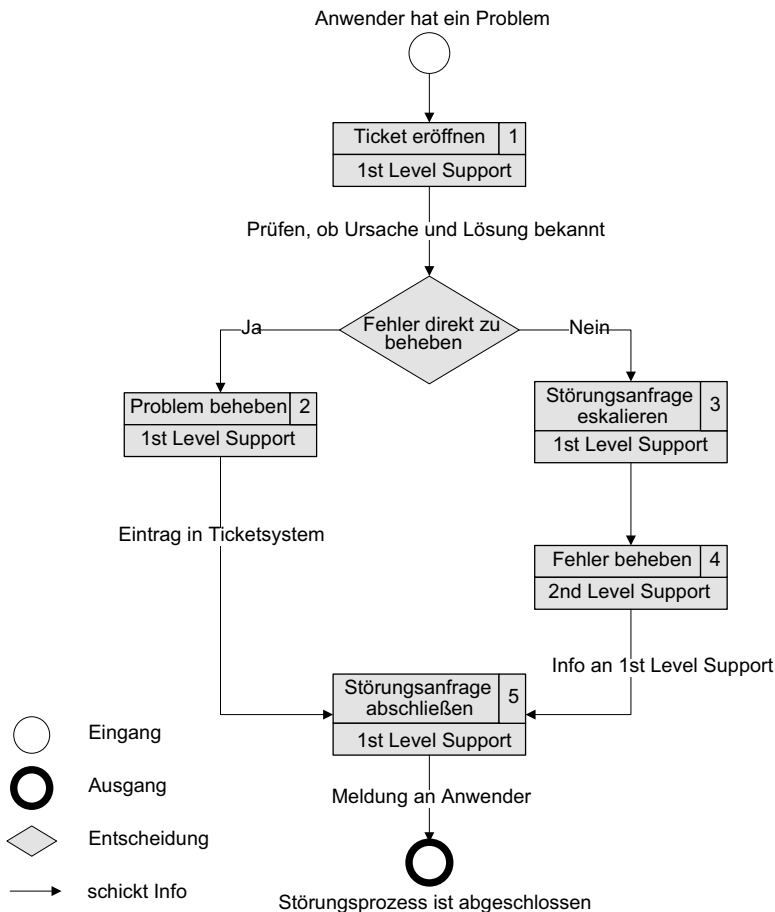


Bild 3.11 Beispielprozess in KSA-Notation

3.4.4.4 Grundlegende Empfehlungen für die Prozessdokumentation

Vor der Wahl eines Prozessmodells für die Dokumentation von Prozessen ist es wichtig zu klären, welchen Einsatzzweck die Dokumentation hat und in welchem Kontext sie benötigt wird. Steht bei der Dokumentation der Prozesse die ISO-Zertifizierung im Vordergrund, ist ein anderer Abstraktionsgrad erforderlich, als wenn die Prozessdokumentation in erster Linie die Mitarbeiter bei der Erledigung ihrer Aufgaben unterstützen soll. Und werden Prozessdokumentationen als Grundlage für die Implementierung automatisierter Abläufe benötigt, sind wiederum andere Anforderungen zu berücksichtigen, da in diesem Fall die Frage der Standardisierung im Vordergrund stehen muss.

Von der Zielsetzung der Prozessdokumentation hängt nicht nur die Auswahl der Methode, sondern auch deren Inhalt und Detaillierungsgrad ab. Die Festlegung der Notation ist in der Praxis außerdem häufig mit der Einführung eines Tools zur Prozessmodellierung verknüpft. An dieser Stelle sollen daher nur einige grundsätzliche Hinweise gegeben werden.

EPKs bieten als quasistandardisiertes Modellierungsmodell den Vorteil, dass Konventionen für die Prozessmodellierung im Unternehmen einfacher durchgesetzt werden können und diese allgemeingültig sind. Außerdem können erstellte Prozesse bei einer späteren Einführung eines Prozessmodellierungstools übernommen werden. Allerdings bedingt die Struktur der EPKs, dass sich komplexe Prozesse oder Arbeitsabläufe nur schwer darstellen lassen. Zum einen werden EPKs in diesen Fällen sehr lang, da für alle Funktionen dargestellt werden muss, durch welche Ereignisse sie initiiert werden, und zum anderen sind Verzweigungen und Schleifen nur schwer darstellbar.

Flussdiagramme sind im Gegensatz zu EPKs gut zur Darstellung komplexer Prozessabläufe geeignet. Die Prozessmodellierung mit Flussdiagrammen wird, weil sie weniger starren Regeln unterliegt, häufig als einfacher empfunden. Diese Darstellungsart ist somit zur Modellierung operativer Arbeitsabläufe meist besser geeignet als EPKs. Aus den beschriebenen Vor- und Nachteilen beider Notationen lässt sich fast zwangsläufig ableiten, dass eine Kombination ein sinnvoller Weg sein kann. Während EPKs oder eEPKs zur Modellierung der Prozesse auf einer abstrakten Ebene eingesetzt werden, erfolgt die Darstellung der operativen Arbeitsabläufe in Form von Flussdiagrammen.

Zur Darstellung von Prozessen im Rahmen des Qualitätsmanagements kann auch die Verwendung der KSA- oder RACI-Notation sinnvoll sein. Zur Modellierung der operativen Arbeitsabläufe ist allerdings auch hier die Verwendung von Flussdiagrammen zu empfehlen.

Unabhängig vom verwendeten Modellierungsmodell ist es sinnvoll, verbindliche Richtlinien für die grafische Darstellung von Prozessen einschließlich Benennungen festzulegen und dabei die folgenden Aspekte zu regeln:

- Verwendung der grafischen Symbole (insbesondere bei Verwendung von Flussdiagrammen und eEPKs)
- Darstellung der ausführenden Rolle im Diagramm mittels Symbol oder durch Verwendung von Funktionsbändern
- Nummerierung der Objekte. Hier gilt es u. a. festzulegen, ob nur Tätigkeiten zu nummerieren sind oder beispielsweise auch Dokumente, Datenspeicher, Entscheidungen und Unterprozesse.

Die Bedeutung der Symbole muss in jedem Dokument in einer Legende dargestellt werden. Dies ist wichtig, um sicherzustellen, dass der Ersteller des Prozesses und der Anwender das Gleiche sehen, also das gleiche Verständnis von den verwendeten Symbolen haben.

Ein wichtiger und schwieriger Punkt ist der anzuwendende Detaillierungsgrad. Bei der Modellierung der Abläufe stellt sich meist die Frage, wie genau diese modelliert werden sollen. Einerseits möchte man eine möglichst genaue Modellierung, um Mehrdeutigkeiten auszuschließen, andererseits möchte man die Modelle klein halten, um Übersichtlichkeit zu gewährleisten. An dieser Stelle kann nur auf die Ausgangsfrage verwiesen werden: Was ist der Einsatzzweck und wer ist die Zielgruppe? Der Detaillierungsgrad muss an dieser Frage ausgerichtet werden.

Hilfreich ist hierbei eine mehrstufige Vorgehensweise, d. h. eine Unterteilung in Haupt- und Unterprozesse und eine Verfeinerung einzelner Aufgaben in gesonderten Arbeitsabläufen. In der Prozessbeschreibung kann dann auf die Detailbeschreibungen verlinkt werden. Eine Verfeinerung der Prozesse auf mehreren Ebenen ermöglicht es, alle Modelle einer Ebene möglichst gleich granular darzustellen und trotzdem einzelne Prozesse stärker zu verfeinern.



Hilfreiche Vorlagen

Das Bundesverwaltungsamt stellt auf seiner Internetseite www.bva.bund.de eine Reihe hilfreicher Anleitungen zur Prozessdokumentation zur Verfügung (beispielsweise das Konventionenhandbuch für eine einheitliche Modellierung von IT-Prozessen und Diensten). [Bundesverwaltungsamt, 2013]

3.4.5 Prozesslandkarte zur Darstellung der Verzahnung von Fachbereichen und IT

Zusätzlich sind die Erstellung und Pflege einer IT-Prozesslandkarte zu empfehlen. Eine Prozesslandkarte dient der grafischen Darstellung der Wechselwirkungen und/oder zeitlichen Beziehungen der Prozesse einschließlich des Zusammenwirkens der einzelnen Teilprozesse. Was für die Darstellung der Aufbauorganisation das Organigramm ist, das ist für die Ablauforganisation die Prozesslandkarte. Sie dient originär der Darstellung der Geschäftsprozesse, kann aber auch zur grafischen Abbildung der IT-Prozesse nützlich sein.

Ihre Publikation soll auch dazu beitragen, dass die Mitarbeiter und Führungskräfte die Einordnung „ihres“ Prozesses in das Gesamtgefüge erkennen und so die Bedeutung ihrer Leistung beurteilen können. Sie enthält aber weder Informationen zu den Prozessen selbst noch Input-Output-Informationen noch Informationen bezüglich der Prozessschrittabfolge.

Bei einer HTML-basierter Bereitstellung der Prozessdokumentation ist es sinnvoll, die Prozesslandkarte als Einstiegsseite bzw. Inhaltsübersicht zu verwenden und diese mit den dahinterliegenden Prozessen für einen direkten Zugriff zu verknüpfen.

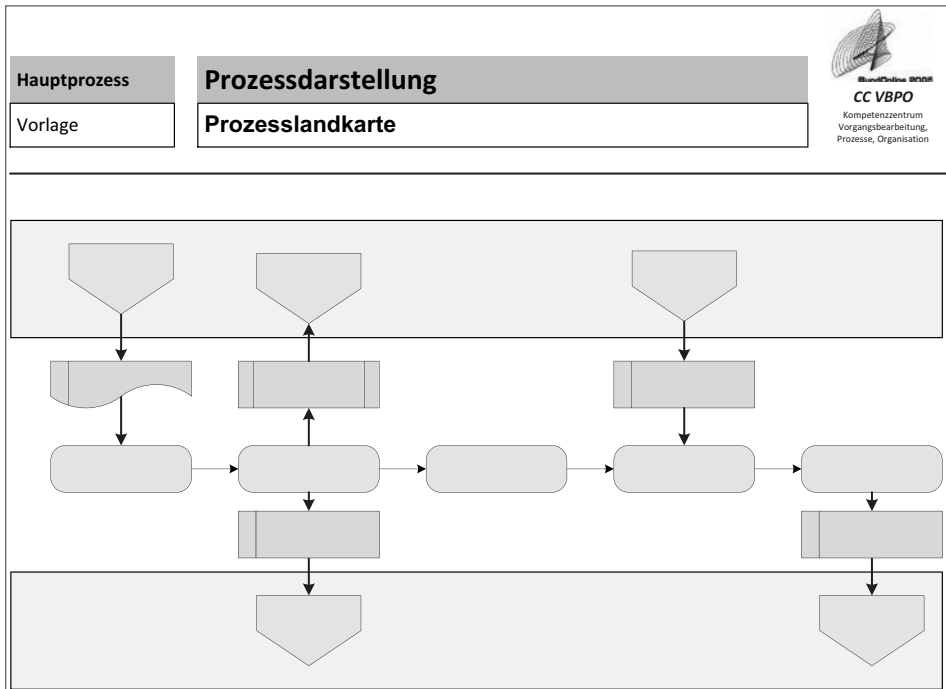


Bild 3.12 Vorlage für eine Prozesslandkarte. Quelle: Bundesverwaltungsamt [2013]

Welche und wie viele Ebenen dargestellt werden, wird durch das individuelle Prozess- und Dienstmodell und durch das verwendete Prozessmodellierungsmodell bestimmt. Die Form der Modellierung hängt stark von den jeweiligen Einsatzgebieten des Modells ab. Zur Abbildung fachlicher und zugehöriger informationstechnischer Sachverhalte finden in der Praxis unterschiedliche Modellierungsstandards Anwendung. Der Grund dafür ist, dass fachliche und technische Modelle auf sehr unterschiedliche Weise genutzt werden, da Fachseite und IT unterschiedliche Ziele bei der Modellierung verfolgen. Häufig erstellen Fach- und IT-Verantwortliche voneinander unabhängige Modelle, ohne diese miteinander abzugleichen.

Dabei wäre eine Zusammenfassung fachlicher und technischer Inhalte in einem Modell durchaus wünschenswert, um ein gemeinsames Verständnis aller Betroffenen zu erreichen. Hilfreiche Hinweise zur Verzahnung von Fach- und IT-Prozessen und zum Aufbau eines integrierten Prozessmodells bietet eine entsprechende Broschüre des Bundesverwaltungsamts. Die möglichen Modellierungsebenen und die strukturellen Zusammenhänge in einem solchen Modell zeigt Bild 3.13.

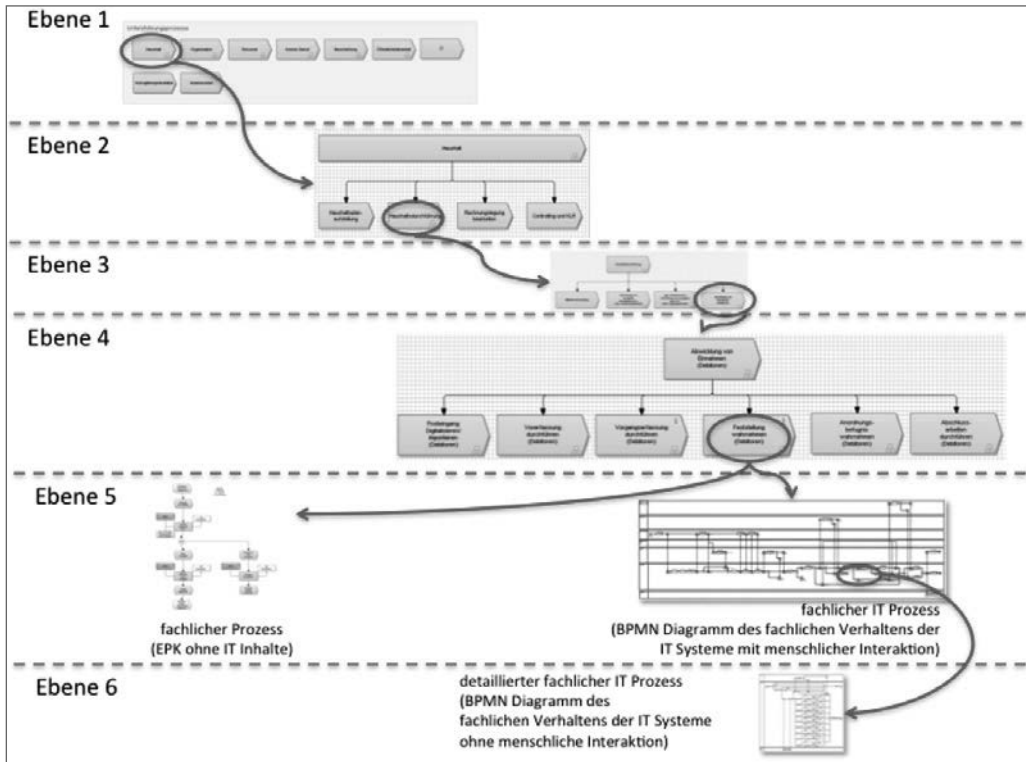


Bild 3.13 Kombiniertes Modellierungsmittel zur Abbildung der Verzahnung von Geschäfts- und IT-Prozessen. Quelle: Bundesverwaltungsamt [2012]

3.4.6 Rollenkonzept

Mit der Einführung des ersten Prozesses wird zusätzlich eine Dokumentation der Rollen erforderlich. Rollen werden innerhalb von Prozessen verwendet, um Verantwortlichkeiten sowohl für den Prozess als auch für die einzelnen Tätigkeiten innerhalb eines Prozesses festzulegen. Um eine allgemeingültige Verwendung aller Rollen innerhalb des Unternehmens bzw. der IT-Organisation zu gewährleisten, ist die Pflege eines sogenannten *Rollenkonzepts* zu empfehlen. Sinnvollerweise sollte auch eine *Betriebsmatrix* gepflegt werden.

Für das Funktionieren der IT-Prozesse ist das IT-Rollenkonzept von besonderer Bedeutung. Während beim funktionsorientierten Ansatz Rechte und Pflichten einzelnen Mitarbeitern zugewiesen werden, werden beim prozessorientierten Ansatz *Rollen* verwendet. Eine Rolle kann dabei als die Beschreibung einer Menge von Aufgaben und Verantwortlichkeiten definiert werden, die von einem, aber auch von mehreren Mitarbeitern wahrgenommen werden können.



Beispiel: Rollenbeschreibung

Ein Beispiel ist die Rolle „Support-Mitarbeiter“: Ein Mitarbeiter, der diese Rolle innehat, soll bestimmte Aufgaben erfüllen und benötigt bestimmte Rechte und Befugnisse, um seine Aufgaben erfüllen zu können. So ist der Inhaber dieser Rolle beispielsweise befugt, Störungen anzunehmen und Störungsmeldungen im Ticket-System einzutragen.

In der Beschreibung der Rolle muss also genau festgelegt sein, was ein Support-Mitarbeiter überhaupt ist, welche Tätigkeiten er auszuführen hat, welche Befugnisse er hat und welche fachlichen und persönlichen Fähigkeiten für die Ausübung der Rolle erforderlich sind. In der Prozessbeschreibung für die Annahme und Abwicklung von Störungen wiederum steht als Bearbeiter nicht der Mitarbeiter XY, sondern die Rolle „Support-Mitarbeiter“. Dies gewährleistet die Unabhängigkeit von organisatorischen und projektspezifischen Rahmenbedingungen.

Je nach Ausrichtung des Unternehmens kann es ein unternehmensweites Rollenkonzept geben und/oder ein IT-Rollenkonzept, das alle im Bereich der IT eingesetzten Rollen definiert und beschreibt. Bei konsequenter Anwendung (jede Rolle in einem Prozess muss zunächst im Rollenkonzept dokumentiert werden) verhindert ein Rollenkonzept, dass in Prozessen beliebige und nicht im Gesamtsystem verankerte Rollen benannt werden (siehe hierzu auch Abschnitt 3.4.4.4).

In einem weiteren Schritt können die Mitarbeiter des Unternehmens bzw. die Organisationseinheiten den definierten Rollen zugeordnet werden. Wechselt beispielsweise ein Mitarbeiter des Backup-Teams in eine andere Abteilung, wird ihm lediglich die Rolle *Backup-Operator* entzogen. Entsprechend seiner neuen Rolle in der neuen Abteilung können dem Mitarbeiter anhand des Rollenkonzepts alle erforderlichen Kompetenzen und Berechtigungen zugewiesen werden, ohne dass eine Änderung der Prozessdokumentation erforderlich ist. Lediglich die IT-Betriebsmatrix muss angepasst werden.

Die Zielgruppe für das Rollenkonzept sind u. a. die Organisationsverantwortliche sowie die für das Personalmanagement verantwortlichen Mitarbeiter, aber auch Abschlussprüfer und Revisoren. Zwar müssen jedem Mitarbeiter die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein, doch ist dies eine Aufgabe der Verfahrensbeschreibungen und nicht des Rollenkonzepts.

Für die Servicemanagementprozesse lohnt sich ein Blick auf das Rollenmodell von ITIL[®], da für diese Prozesse bereits zahlreiche Dokumentationen vorliegen, die als Vorlage dienen können. Die in ITIL[®] beschriebenen Prozesse definieren jeweils einen Prozesseigner, der die Zielvorgaben und die Kontrolle des Prozesses verantwortet, einen Prozessmanager, der für die Umsetzung des Prozesses verantwortlich ist, und einen oder mehrere Servicetechniker für die operative Umsetzung des Prozesses.

Wie beschrieben, sind im Prozesssteckbrief der Prozessverantwortliche und alle beteiligten Rollen zu benennen. ITIL[®] definiert für die beschriebenen Prozesse jeweils einen *Prozesseigner* (engl. *Process Owner*), der die Zielvorgaben und die Kontrolle des Prozesses verantwortet und für das Erreichen seiner Leistungsziele verantwortlich ist. Zusätzlich gibt es für

jeden Prozess eine oder mehrere Rollen, die für die operative Umsetzung des Prozesses verantwortlich sind (*Prozessnutzer*).

Beispiel Prozessrollen

Typische Aufgaben der beiden Rollen Prozesseigner und Prozessnutzer zeigt beispielhaft Tabelle 3.4.

Tabelle 3.4 Beispiel – Beschreibung von Prozessrollen

Rolle	Zuständigkeiten
Prozesseigner (Verantwortlicher des Prozesses)	<ul style="list-style-type: none"> ▪ Gesamtverantwortung für den Prozess ▪ Klärung der Schnittstellen zu anderen Prozessen ▪ Bewertung und Freigabe des Prozesses ▪ Bewertung der Prozessrisiken und der Maßnahmen zur Risikoreduzierung ▪ Turnusmäßige Überprüfung des Prozesses hinsichtlich Zielerreichung und Effizienz anhand der Prozesskennzahlen und gegebenenfalls Anpassung des Prozesses ▪ Erstellung und Pflege der Prozessdokumente ▪ Turnusmäßige Überprüfung der Prozessdokumente ▪ Bereitstellung der Prozessdokumente (z. B. im Intranet) ▪ Mithilfe bei der Schulung im Umgang mit den Dokumenten ▪ Überprüfung und Abnahme von prozessergänzenden Dokumenten (Arbeitsanleitungen, Formulare, Checklisten usw.)
Prozessnutzer (Prozessausführende)	<ul style="list-style-type: none"> ▪ Ausführung der im Prozess definierten Tätigkeiten ▪ Einhaltung der Vorgaben ▪ Einreichung von Optimierungsvorschlägen zum Prozess beim Prozessmanager ▪ Melden von Problemen, die im Rahmen der Prozessausführung auftreten ▪ Erstellung der prozessergänzenden Dokumente

Beispiel Rollenbeschreibung

Die folgende Tabelle 3.5 zeigt exemplarisch ein Beispiel für die Beschreibung einer Rolle. Zu beachten ist, dass bei dem Beispiel die Art der Dokumentationsmöglichkeit im Vordergrund steht und der Inhalt nur exemplarisch ist.

Der Service Desk wird im Allgemeinen als Anlaufstelle definiert, an die sich die IT-Nutzer mit Problemen und Serviceanfragen wenden können. Der Service-Desk-Manager stellt sicher, dass die im Rahmen des Service Desk definierten Tätigkeiten durchgeführt werden. Eine Rollenbeschreibung für den Service-Desk-Manager kann wie folgt aussehen:

Tabelle 3.5 Beispiel – Rollenbeschreibung

Rollenbeschreibung: Service-Desk-Manager	
Kurzbeschreibung	<ul style="list-style-type: none"> ▪ Der Service-Desk-Manager hat die Gesamtverantwortung für die definierten Service-Desk-Leistungen. Er berichtet an den Service-Desk-Owner. ▪ Der Service-Desk-Manager repräsentiert und führt den Service Desk. Er ist Ansprechpartner für den operativen Betrieb aus Kundensicht.
Aufgaben/Verantwortung	<ul style="list-style-type: none"> ▪ Gesamtverantwortung für den Service Desk ▪ Ansprechpartner für alle Support-Themen aus dem Anwenderbereich ▪ Ansprechpartner im Eskalationsfall ▪ Qualitätsmanagement und Reporting ▪ Liefert regelmäßige Statusberichte über Leistungen und Trends im Service Desk ▪ Führt Reviews durch, welche die Effizienz und Effektivität des Service Desk periodisch untersuchen (Kostenmanagement) ▪ Definiert und führt qualitätssichernde Maßnahmen durch ▪ Informiert den Service-Desk-Eigner über bevorstehende Maßnahmen und Tätigkeiten ▪ Ressourcen- und IT-System-/Infrastrukturmanagement ▪ Organisation und Bereitstellung der notwendigen Technologien und Werkzeuge am Service Desk ▪ Bereitstellung der benötigten Mitarbeiter und Organisation von Trainings
Befugnisse	<ul style="list-style-type: none"> ▪ Stellt die Personalplanung sicher und trägt fachliche Verantwortung für das Personal ▪ Veranlasst Ausbildungs- und Bedarfsplanung ▪ Führt Mitarbeiter- und Bewerbungsgespräche
Anforderungen (technische Fähigkeiten)	<ul style="list-style-type: none"> ▪ Kenntnisse über eingesetzte IT-Systeme (Hardware und Software) ▪ Produktkenntnisse insbesondere des verwendeten Service-Desk-Ticket-Systems ▪ Gute Kenntnisse über die unternehmensspezifische IT-System-/Infrastrukturlandschaft des Unternehmens
Anforderungen (nichttechnische Fähigkeiten)	<ul style="list-style-type: none"> ▪ Kundenorientierung und Kommunikationsfähigkeit ▪ Sicheres Auftreten ▪ Ausgeprägte Präsentationsfähigkeiten ▪ Teamfähigkeit ▪ Durchsetzungsvermögen ▪ Selbstständiges Arbeiten ▪ Organisationsfähigkeit und Zeitmanagement
Unterstützung durch	<ul style="list-style-type: none"> ▪ Alle Rollen aus dem Supportbereich

3.4.7 Betriebsmatrix

Zusätzlich zum Rollenkonzept muss es ein Dokument geben, in dem die Zuordnung von Organisationseinheiten und Personen zu den Rollen erfolgt, also ein Dokument, in dem konkret steht, welcher Rolle der Mitarbeiter XY zugeordnet ist. Dabei kann eine Person mehrere Rollen besetzen; ebenso kann aber auch eine Rolle von mehreren Personen eingenommen werden. Hierfür wird häufig eine sogenannte *Betriebsmatrix* verwendet. Sie definiert die organisatorische Platzierung der Aufgaben und Rollen. Eine Betriebsmatrix ermöglicht demzufolge eine eindeutige Zuordnung von Personen und Rollen und hilft dabei, Doppelbesetzungen, unklare Zuständigkeiten und Überschneidungen zu verhindern. Zeigt sich beispielsweise bei der Erstellung, dass ein Mitarbeiter Rollenträger für sehr viele Rollen ist, sollte überprüft werden, ob nicht einzelne Rollen auf andere Mitarbeiter übertragen werden können. Dies ist insbesondere dann notwendig, wenn für einzelne Rollen eine Funktionstrennung vorgesehen ist. Zwar ist es durchaus üblich, dass ein Mitarbeiter mehrere Rollen ausübt, doch wenn dieser Inhaber dreier Rollen ist, die eigentlich jeweils 100 Prozent seiner Arbeitszeit beanspruchen, so stimmt etwas nicht. Möglicherweise wird dabei aber auch deutlich, dass wichtige Rollen überhaupt nicht eindeutig zugeordnet sind und im operativen Betrieb „irgendwie von irgendjemandem“ erledigt werden.

Die Betriebsmatrix kann ebenfalls entweder zentral für das gesamte Unternehmen gepflegt werden oder auch gesondert von jeder Organisationseinheit. In den meisten Unternehmen gibt es zwar Dokumente, aus denen hervorgeht, welcher Mitarbeiter welche Position einnimmt. Eine rollenbasierte Betriebsmatrix ist aber noch eher selten zu finden. Fehlt also eine solche Betriebsmatrix, ist die Erstellung einer Matrix zu empfehlen.

Die nachstehende Tabelle 3.6 zeigt beispielhaft einen Auszug aus einer Betriebsmatrix für den IT-Betrieb.

Tabelle 3.6 Beispiel Betriebsmatrix

Rolle	Name Rollenträger	Organisatorische Zuordnung	Anmerkungen
Rollen im Supportprozess			
Prozess-Owner	Mitarbeiter A	Bereichsleiter XY	Rollenzuständigkeit endet am 31. 12. 20xx
Service-Desk-Manager	Mitarbeiter B	Gruppenleiter XY	
Incident Manager	Mitarbeiter K	Organisationseinheit XY	
1st Level Support	Mitarbeiter L	Organisationseinheit XY	
	Mitarbeiter M	Organisationseinheit XY	Zu 30 % zugeordnet
	Mitarbeiter N	Organisationseinheit XY	
	Mitarbeiter O	Organisationseinheit XY	
2nd Level Support	Mitarbeiter M	Organisationseinheit XY	Zu 70 % zugeordnet
	N. N.	Externer Berater	

(Fortsetzung nächste Seite)

Tabelle 3.6 Beispiel Betriebsmatrix (Fortsetzung)

Rolle	Name Rollenträger	Organisatorische Zuordnung	Anmerkungen
Rollen im Change-Management-Prozess			
Prozess-Owner	Mitarbeiter A	Bereichsleiter XY	Rollenzuständigkeit endet am 31. 12. 20xx
Change- Manager	Mitarbeiter C	Gruppenleiter XY	
Change-Operator	Mitarbeiter D	Organisationseinheit XY	
	Mitarbeiter E	Organisationseinheit XY	
	Mitarbeiter F	Organisationseinheit XY	

Index

A

Abbildungen
– Beschriftung 416
– verankern 426
– Verzeichnis 417, 419
Abbildungsverzeichnis 415
Abgabenordnung 17, 305
Ablaufbeschreibungen 55 f., 123, 127 f.
Ablaufdiagramm 81, 145
Abnahmetest 178
Adobe Acrobat 427, 436
Aktivität 56, 126, 352
Änderungsanforderung 352
Änderungsantrag 148
Änderungsmanagement 147, 352
Änderungsprozess 148
Anforderungsdokumentation 165
Anforderungsspezifikation 172
Anonymisierung 247
Anwendungen 109, 121
Anwendungsarchitektur 176
Anwendungsbetrieb 157, 164, 184
Anwendungsbetrieb und -entwicklung 9
Anwendungsdokumentation 3, 112, 157
Anwendungsentwicklung 157, 164
Anwendungshandbücher 336
– Inhalte 337 f.
Anwendungsklassifizierung 159 f.
Anwendungslandschaft 310
Anwendungsmanagement 158
Anwendungssoftware 107
Application Lifecycle Management 164
Arbeitsanleitungen 56, 80, 126, 128 ff.
Arbeitsanweisungen 128, 352
Arbeitsdokumentation 430
Architekturdokumentation 176
Archivierung 305, 307, 311, 313

Aufbewahrungsfristen 17, 314
Auftragsdatenverarbeitung 249 f.
Auftragsverarbeitungsverträge 251
Aufzeichnungen 57, 121, 306, 353
Authentizität 214
Automatisierte Inventarisierung 133, 316
Autorisierung 214
Availability Management 141

B

Backstage-Bereich 404
BaFin *siehe* Finanzdienstleistungsaufsicht
BAIT 33 f.
Barrierefreie Dokumente 439
BCM *siehe* Business Continuity Management
BDSG-2018 *siehe* Bundesdatenschutzgesetz
BDSG-neu *siehe* Bundesdatenschutzgesetz
Berechtigungshistorie 118
Berechtigungskonzept 134 f., 353
Berechtigungsmatrix 135 f., 353
Berichtsplan 200
Beschriftungen 416
Betriebs- und Steuerungstechnik 116
Betriebsdokumentation 8 f., 11 f., 66, 68 ff.
Betriebshandbuch 182, 353
Betriebsmatrix 91 f., 95, 353
Betriebsübergabe 184
Bimodale IT 10
BITKOM 245, 251
Bitkom Kompass 371
British Standards Institution 255, 441
BS 25777 255
BSI 34, 36
BSI-Baustein Notfallmanagement 255
BSI-Gesetz 26, 36
BSI-Standards 217 f.
– Standard 100-4 218, 252, 296

- Standard 200-1 218
- Standard 200-2 218
- Standard 200-3 218, 235 f.
- Standard 2000-1 220
- Standard 2000-2 220
- Standard 2000-3 220
- Bundesamt für Sicherheit in der Informations-
technik *siehe* BSI
- Bundesdatenschutzgesetz 21, 243, 368
- Business-Anwendungen 110
- Business Continuity Management 142, 218, 237,
254, 259
 - Dokumentation 260
- Business Continuity Plan 278
- Business-Impact-Analyse 237, 258, 263 f., 267
- Business Map 428
- Business Process Management 318
- Business Process Modeling Notation
siehe Prozessdokumentation

C

- Capability Maturity Model Integration 63
- Capacity Management 141, 147
- Change-Management 140, 147
- Change-Prozess 146
- Change Request 147 ff.
 - Bericht 192
- Checklisten 132
- Client-Anwendungen 109
- CMDB *siehe* Configuration Management
Database
- CMMI 364
- Common Assessment Framework 363
- Compliance 14, 325, 355
- Configuration Items 153, 319
- Configuration Management Database 70, 134,
153 f., 308, 318 f., 322
- Configuration Management System 319
- Continual Service Improvement 143
- Controls *siehe* Sicherheitsmaßnahmen

D

- Dashboard Map 431
- Datenschutz 215, 314 f., 353
- Datenschutzdokumentation 237
- Datenschutzgrundverordnung 21 f., 98, 237
- Datensicherheit 19, 215, 353
- Definition IT-Dokumentation 1
- Deployment Management 140
- Designdokumente 172
- Detaillierungsgrad 2

- Deutsches Institut für Normung e. V.
siehe Normierungsorganisation
- Dienstleistungsbeschreibung 76
- DIIR-Standards 43, 202
- DIKW-Modell 321
- DIN 69901 187, 189 f., 201, 392
- DIN-Standards *siehe* Standards
- Documented information *siehe* Dokumentierte
Informationen
- Document Lifecycle Management 303
- Dokumentation 354
- Dokumentationsanforderungen 15, 17, 20, 22, 24,
41, 47, 53, 184, 239 ff.
- Dokumentationsarchitektur 291
- Dokumentationsbereiche 7 f., 11 f.
- Dokumentationskonzept 293
- Dokumentationslösungen 309
- Dokumentationsmanagement 287 f., 293, 301, 354
- Dokumentationsmanagementsystem 289
- Dokumentationsmanager 293
- Dokumentationsplattform 313
- Dokumentationsrichtlinie 289, 291, 293, 354
- Dokumentationsstruktur 3 f., 9 f., 51
- Dokumentationsverfahren 293, 310
- Dokumentationsvorgaben 290
- Dokumente 57, 353
- Dokumenteigenschaften 405 f.
- Dokumenterstellung
 - Abhängigkeiten 344
 - Abstraktionsgrad 343
 - Dokumentenumfeld 343
 - Gliederung 345
 - Mitgeltende Dokumente 344
 - Recherche 342
 - Visualisieren 344
 - Vorgaben 343
 - Vorgängerversionen 344
 - Zielgruppe 343
- Dokumentinformationen 406
- Dokumentvorlagen 410, 417
- Dokumentenablage 296
- Dokumentenklassen 294, 354
- Dokumentenlayout 299
- Dokumentenlebenszyklus 303, 306
- Dokumentenlenkung 123
- Dokumentenmanagement 288 f., 310, 354
- Dokumentenmanagementsystem 211, 296, 310 f.,
314
- Dokumentenmatrix 294
- Dokumentenreview 348 f.
- Dokumententyp 294 f., 354
- Dokumentenverwaltung 289, 301
- Dokumentierte Informationen 37, 57 f., 289, 354

DSGVO *siehe* Datenschutzgrundverordnung
 DSGVO Erwägungsgründe 369
 DV-Konzept 53

E

Eingabekontrollen 246
 Eingebettete Systeme 116
 Energiewirtschaftsgesetz 27
 Enterprise Architecture Management 309
 Enterprise Content Management 310
 Entscheidungsvorlage 355
 EPK-Notation 317
 Ereignisgesteuerte Prozessketten 82f., 88
 – eEPKs 83
 – Erweiterte EPKs 83
 – Notation 83
 Ergebnisdokumente 358
 Ergebnistypen agile Softwareentwicklung 185
 Ergebnistypen klassische Softwareentwicklung 166
 Erklärung zur Anwendbarkeit 222
 Ersatzbeschaffungsmaßnahmen 278
 EU-Datenschutzgrundverordnung
siehe Datenschutzgrundverordnung

F

Fachanwendungen 101, 112f., 160, 309, 355
 Fachausschuss für Informationstechnologie (FAIT) 39
 Fachkonzept 167
 Fachverfahren *siehe* Verfahren
 Facility 113
 – Facility Management 113
 – Gebäudemanagement 113
 Feldfunktionen 405
 Financial-Management 141
 Finanzdienstleistungsaufsicht 29f.
 FitSM 155f.
 Flussdiagramme 81, 84, 88
 Flussdiagrammnotation 84
 Formatierungen 410
 Formatvorlagen 410, 413f., 418, 422
 – Inhaltsverzeichnis 417f.
 – Standardformatvorlage 410
 – Überschriften 412
 – Verzeichnisse 422
 Formelverzeichnis 419
 Formulare 131f.
 Freigabeverfahren 303
 Führungsprozesse 195
 Funktion 2, 65

Funktionsorientierung 6
 Funktionstests 282

G

GAMP 29
 GDPdU *siehe* GoBD
 Geschäftsfortführungsplan 31, 269, 276, 278, 355
 Geschäftsprozesse 6
 Gesetze 15
 Gesetzeskonforme Archivierung 314
 Gliederungsebenen 413
 Glossar 291, 300, 351
 GoBD 18f., 44, 163, 305
 GoBS *siehe* GoBD
 Good Laboratory Practice 28
 Good Practice Guidelines 257
 Governance 325
 GRC-Dokumentation 325
 GRC-Management 355
 GRC-Werkzeuge 325
 Grundschutzbausteine 102
 Grundschutzhandbuch 217f.
 Grundschutz-Kataloge 218, 255

H

Handelsgesetzbuch 16f., 305
 HERMES 393
 Hostsystem 108

I

IDW Prüfungsstandards 39
 – PH9.330. 39
 – PS 330 39
 – PS 850 39f.
 – PS 880 39f.
 – PS 951 40
 IDW PS 330 40
 IDW PS 951 41
 IEEE-Standard 829 178, 401
 Incident 140
 Incident-Management 139, 151
 Index 420f.
 Indexeinträge 420f.
 Industrial Control Systems 116
 Industrielle IT 116f.
 Information 215
 Information Security Management 216
 Informationssicherheit 215
 Informationssicherheitsdokumentation 213, 323
 Informationssicherheitsleitlinie 222, 231

- Informationssicherheitsmanagement 213
 - Informationssicherheitsprozess 222
 - Infrastruktur 113
 - Inhaltsspezifische Dokumententypen 295
 - Inhaltsverzeichnis 417, 419
 - Institut der Wirtschaftsprüfer 39
 - Integrität 17, 214, 315
 - Internes Kontrollsystem 19, 50
 - Interne Revision 31
 - Inventarisierungsanwendungen 316
 - ISIS 12 374
 - ISMS *siehe* Informationsmanagementsystem
 - ISO 27001 Dokumentation 221
 - ISO-Normen *siehe* Normen
 - ISO 9001 34
 - ISO 20000 60 f., 257
 - ISO 22301 256
 - ISO 22313 256
 - ISO 27000 256
 - ISO 27001 216
 - ISO-27001 216
 - ISO 27002 217, 224
 - ISO 27005 217, 235
 - ISO 31000 235
 - ISO-Redline 61
 - IT-Anwendungen 113, 121, 160, 355
 - IT-Aufbauorganisation 9, 137
 - IT-Betrieb 357
 - IT-Betriebsdokumentation 97, 355
 - IT-Compliance 14, 50
 - IT-Dokumentation 356
 - IT-Dokumentationskonzept 291
 - IT-Governance 50, 325
 - IT-Governance-Prozesse 50
 - IT-Grundschatz 36, 100, 216, 254
 - IT-Grundschatz-Bausteine 219
 - IT-Grundschatzdokumentation 225
 - IT-Grundschatz-Kompodium 102, 105, 123, 159, 219, 225
 - IT-Infrastruktur 100, 115
 - IT-Konzept 53 f., 356
 - IT-Management 8, 50, 52
 - IT-Notfalldokumentation 357
 - IT-Notfallhandbuch 357
 - IT-Organisation 51, 53, 55, 65
 - IT-Planungsrat 380
 - IT-Projekt 204, 358
 - IT-Prozesse 7
 - IT-Prüfungen 43
 - IT Security Management 141, 443
 - IT-Service 59, 64, 66 f., 73, 356
 - IT-Service Continuity Management 142, 259, 267, 356
 - IT-Service Continuity Plan 278
 - IT-Servicedokumentation 67
 - IT-Serviceerbringung 99
 - IT-Servicekatalog 74
 - Business-Servicekatalog 75
 - Technischer Servicekatalog 75
 - IT-Servicemanagement 59, 64, 76, 137, 139, 146, 257, 318, 356
 - IT-Servicemanagementdokumentation 318
 - IT-Servicemanagement-Prozesse 139, 142, 144 f.
 - IT-Sicherheit 215
 - IT-Sicherheitsgesetz 25
 - IT-Sicherheitskatalog 27 f.
 - IT-Sicherheitskonzept *siehe* Sicherheitskonzept
 - IT-Strategie 53
 - IT-Strategiemanagement 53
 - IT-System 105, 120, 356
 - IT-System-/Infrastrukturbetrieb 9, 98 f.
 - ITIL® 60, 92, 125, 137, 146
 - ITIL®-Prozesse 139, 144
 - ITSM *siehe* IT-Servicemanagement
 - IuK-Mindestanforderungen 209, 362
- ## J
- Jahresabschlussprüfung 39, 41 f.
- ## K
- Katastrophe 266
 - Kennzeichnungspflichten 296
 - Bearbeitungsnummer 298
 - Bearbeitungsstatus 297 f.
 - Dokumentennummer 297
 - Versionierung 297
 - Versionsnummer 298
 - Kernprozesse 6
 - Knowledge Management 321
 - Known Error Database 152, 322
 - Kommunikationsanwendungen 111
 - Kommunikationspläne 275
 - Kommunikationsstrukturanalyse 87
 - Konkordanzdatei 421
 - Kontinuitätsstrategien 264
 - Konzept 126, 192, 357
 - Kreditwesengesetz 29
 - Krise 258, 266
 - Krisenkommunikationsplan 275
 - Krisenmanagement 272
 - Krisenstab 265, 271 ff.
 - Bestandsaufnahme 273
 - Lagebeurteilung 273

Krisenstabsleitfaden 272
 Krisenstabsraum 272
 Kritisverordnung 26
 KWG §44er Prüfung 30

L

Langzeitspeicherung 305
 Lastenheft 167ff.
 Layoutvorschriften 299
 Leistungsschein 74, 76
 Leistungsverzeichnis 168
 Leitlinie für das Notfallmanagement 261
 Lenkung von Aufzeichnungen 306
 Lenkung von Dokumenten 302
 Lesestraßen 415
 Lizenzmanagement 108
 Löschkonzept 240

M

Machbarkeitsstudie 191
 Managementaufgaben 8
 Managementprozesse 6
 Managementsystem 289
 Marginalien 412, 415
 MaRisk 30 f., 269
 – InvMaRisk 30
 – KAMaRisk 30
 – VAMaRisk 30
 Maschinenrichtlinie 162
 MaSI 32 f.
 Meilensteinplan 191
 Metadaten 312, 327
 Methodik zur Risikoeinschätzung 222
 Microsoft Solutions Framework 204
 MindManager 428 f.
 – Business Map 428
 – Hyperlinks 430
 – Multifunktionsleiste 428
 Mindmap 342, 344 f.
 Mitgeltende Dokumente 357
 MSF-Modell 204

N

Nachweisdokumente 224
 Namenskonvention 131, 291, 300
 Namensregeln 301
 Netzbasierte Anwendungen 109
 Netzstrukturplan 28
 Netzwerkkomponenten 113 f.
 Netzwerkmanagement 316

Netzwerkmonitoring 316
 Nichtabstreitbarkeit 214
 Normal.dot 410
 Normen 34 f.
 Normierungsorganisation
 – CEN 35
 – DIN 35
 – IEC 35
 – ISO 35
 Normstruktur 37
 Notation 84
 Notbetrieb 274, 276, 280
 Notfall 258, 266
 Notfallabschluss 274
 Notfallbeauftragter 265
 Notfallbewältigung 252, 260, 269, 271
 Notfalldokumentation 11 f., 251, 323
 Notfallhandbuch 253, 261, 270, 274
 Notfallkonzept 31, 237
 Notfallmanagement 252, 260
 Notfallmanagementanwendung 323
 Notfallmanagementleitlinie 357
 Notfallmanagementprozess 260, 283
 Notfallmanagement-Vorlagen 286
 Notfallorganisation 270
 Notfallplan 358
 Notfallstab *siehe* Krisenstab
 Notfallstandards 252
 Notfalltest 281
 Notfallübung 281
 Notfallvorsorge 260, 269
 Notfallvorsorgekonzept 252, 261 f., 265,
 358
 Notfallvorsorgemaßnahmen 269
 Nutzergruppen 1 f.

O

Objekt
 – einbetten 423, 426
 – einfügen 425
 – Inhalte einfügen 424, 427
 – kopieren 423 f.
 – verknüpfen 424 ff.
 Office Microsoft 404
 Operation Level Agreement 73
 Operative Tätigkeiten 64, 123, 127
 Ordnungsmäßigkeit 17
 Organisationsrichtlinien 30 f.
 Orientierungshilfe Datenschutz 315, 369
 Outsourcing
 – Auftragsdatenverarbeitung 249
 – Dokumentation 231

- Prüfung 40
- Verantwortlichkeiten 68

P

- PCI-DSS 29
- PDCA-Modell 60
- PDF-Datei 436 f.
- PDF-Format 438
- Personalmanagement 92
- Pflichtenheft 167, 171 ff.
- Phasengliederung 204
- Plan-Review 282
- Planungsdokumente 189
- PMBok 202
- Positionsrahmen 415
- PRINCE2 190
- Problemmanagement 140
- Process Maturity Framework 63
- Product Backlog 185
- Produktdokumentation 161
- Produktsicherheitsgesetz 162, 444
- Project Audit Universe 202
- Projekttakte 189, 192 f., 206, 358
- Projektberichte 200
 - Projektabschlussbericht 200
 - Projektsonderberichte 200
 - Statusberichte 200
- Projektdokumentation 11 f., 187 ff., 209
- Projektdokumente 210
- Projekthandbuch 193 f.
- Projektkommunikation 200
- Projektmanagement 187, 201, 392
- Projektmanagement Office 209
- Projektmanagementdokumente 207
- Projektmanagement-Handbuch 190
- Projektmanagementphasen 194, 205 f.
- Projektmanagementprozesse 190, 195 f., 198
- Projektorganisation 189
- Projektphase 204
- Projektsteckbrief 191
- Prototyp 186
- Prozesse 56, 59, 64, 126, 144, 358
 - Prozessbewertung 80
 - Prozesseigner 92
 - Prozesskennzahlen 80
 - Prozessnummerierung 79
 - Prozessnutzer 93
 - Prozessrollen 92
- Prozessbausteine 103, 225, 227, 229
- Prozessbeschreibung 67, 145, 200, 358
 - Ablaufdiagramm 81, 146
 - Funktionsbänder 84

- Inhaltliche Anforderungen 78
- Prozessziele 78
- Steckbrief 79
- Verantwortlichkeiten 78
- Prozessdokumente 145
- Prozessdokumentation 67, 144, 317, 398, 402
 - Detaillierungsgrad 88
 - Empfehlungen 88
 - Modellierungsmodell 88
 - Prozessmodellierungswerkzeuge 81
 - Prozessnotation 81
- Prozessresultatdokumente 359
- Prozesshaus 195
- Prozesslandkarte 79, 89 f., 359
- Prozessmanagement 317 f.
- Prozessmodellierungswerkzeuge 317
- Prozessorientierung 6, 359
- Prozessrollen 93
- Prozesssteckbrief 81, 359
- Pseudonymisierung 247

Q

- Qualitätssicherung 292, 304, 347
 - Checkliste 348 f.
- Querverweise 422
- Querverweisfunktion 422

R

- RACI
 - RACI-Diagramme 85
 - RACI-Notation 86
- Rahmendokumente 11 f., 359
- REACH 28
- Redaktionssysteme 310
- Regelbetrieb 274
- Regelwerke 16
 - rechtlich 16
 - unternehmensextern 16
 - unternehmensintern 16
- Reifegradmodell 63, 73
- Release-Management 140
- Request for Change 146, 148
- Request Fulfillment 140
- Requirements 400
- Requirements Engineering 165, 171
- Ressourcen 65
- Review 359
- Revision 42
- Revisionsicherheit 290, 305
- Revisionsstandard 43
- RFC 148

Richtlinien 16, 359
 Risikoanalyse 258, 263 f., 267
 Risikohandbuch 359
 Risikomanagementdokumentation 234
 Rollen 91 f.
 Rollenbeschreibung 54, 92 f.
 Rollenkonzept 54, 91 f.

S

Schadensszenario 278
 Schnellformatvorlagen-Katalog 413
 Schnittstellendokumente 175
 Schrift
 – Formatvorlage 410
 – Schriftart 411 f.
 – Schriftgröße 410
 – Serifenschrift 411
 – Standardschrift 410
 Schriftlich fixierte Ordnung 16
 Schritt-für-Schritt-Anleitungen 129
 Schulungskonzept 192
 Scoping der IT-Dokumentation 3
 Scrum 185
 Service Asset and Configuration Management 141
 Service Catalogue Management 147
 Service Design 143
 Service Knowledge Management System 321, 444
 Service Level 73
 Service Level Agreements 73
 Service Lifecycle 142
 Service Operation 145
 Service Requests 140
 Service Strategy 142
 Service Transition 143, 145
 Service-Level-Management 140
 Service-Provider 66
 Servicebeschreibung 73 f.
 Servicebetrieb 9, 143
 ServiceDesk 139
 Serviceerbringung 9
 Servicekatalog 67, 356
 SharePoint 326 f.
 – Beispiel IT-Dokumentation 328
 – Beispiel WIKI 336
 – Dokumentenbibliotheken 327
 – Dokumentensteuerung 333
 – Inhaltstypen 332
 – Inhaltsverwaltung 330
 – Konzept 339
 – Listen 327
 – Rechtsstruktur 329
 – Site 327

– Spalten 330
 – Versionsverwaltung 334
 – Websitestruktur 328
 – WIKI-Seitenbibliothek 336
 – Workflows 335
 SharePoint Microsoft 407 f.
 Sicherheitskonzept 224, 232 f., 356
 Sicherheitsmaßnahmen 223
 Sicherheitsrichtlinie 359
 Single Point of Information 119, 327, 336
 SkyDrive 408
 Skydrive Pro 407
 Snagit 433, 435
 Snagit Editor 433
 Snipping Tool 433
 Sofortmaßnahmen 272
 Software as a Service (SaaS) 160
 Softwaredokumentation 161
 Softwareentwicklung 158, 165
 Sollkonzept 172
 Standards 15, 34 f.
 Standard-Clientsystem 102
 Standard-Datenschutzmodell 369
 Standard operating procedures 56, 128
 Standardänderungen 149
 Stand der Technik 26, 249
 Steuerungsprozesse 6
 Störfalldokumentation 151
 Strukturierung 3 f., 9 f., 51
 Strukturierungssicht 4 f.
 Stufenmodell IT-Dokumentation 62 f., 68
 Supportprozesse 6
 Swimlanes 84
 System 100, 360
 Systemakten 67, 101 f., 104, 117 f., 120 ff., 360
 Systemakteninhalte 117
 Systembausteine 100, 103, 226
 Systemdokumentation 67, 100 f., 280, 316, 360
 Systemsicherheit 120
 Systemsoftware 107

T

Tabellen
 – Beschriftung 416
 – Verzeichnis 416 f., 419
 Technische Dokumentation 161 f., 360
 Technische Spezifikationen 175
 Technische und organisatorische Maßnahmen (TOMs) 242, 245 f., 248
 Telemediengesetz 23 ff.
 Test
 – Abnahmetest 178

- Fachtest 177
- Funktionskontrolle 178
- Funktionstest 177
- Integrationstest 178
- Lasttest 178
- Robustheitstest 178
- Stresstest 178
- Testberichte 180
- Testdokumente 148
- Testdokumentation 177, 181, 360
- Testentwurfsspezifikation 180
- Testfallbeschreibung 180
- Testkonzept 192
- Testmanagement 179
- Testplan 179
- Testprotokoll 180
- Testumgebung 109
- Textauszeichnungen 412
- Trennungskontrollen 246
- TÜVIT 37

U

- Übergabeprotokoll 192
- Überschriften 412f.
- Überschriftenformatvorlagen 412f.
- Übungskonzept 281
- Übungspläne 282
- UMRA 284
 - Module 284
- Umsetzungsrahmenwerk 284
- Unified Modeling Language *siehe* Prozessdokumentation
- Unternehmensgesetz 16
- Unterstützungsprozesse 6, 195
- User Stories 186

V

- Veränderungsmanagement 147, 360
- Verfahren 55f., 243, 360
- Verfahrensbeschreibung 45f., 55, 163, 361
- Verfahrensdokumentation 44f., 56, 163, 361

- Verfahrensverzeichnis 243, 361
- Verfügbarkeit 17
- Verfügbarkeitskontrollen 246
- Verknüpfungen 424f.
- Verordnungen 15f.
- Verträge 118
- Vertraulichkeit 214, 315
- Vertraulichkeitsklasse 294
- Vertraulichkeitsstufe 299
- Verweise 426
- Verzeichnis der Verarbeitungstätigkeiten 242ff.
- Virtualisierte Systeme 109
- Virtualisierung 107
- Virtualisierungsumgebung 109
- Virtuelle Akten 312, 361
- Visio Microsoft 317
- V-Modell 204f.
- Vorgängerdokumente 344
- Vorgehensmodelle 204
- Vorgehensmodell IT-Dokumentation 290

W

- Weitergabekontrollen 246
- Wertschöpfungsprozesse 6, 195
- Wiederanlauf 276
- Wiederanlaufplan 253, 274, 276, 278, 361
- Wiederherstellungsplan 278, 361
- Wirtschaftsgrundschutz 219f.
- Wissensmanagement 321
- Word Microsoft 404
- Work Instructions 352
- Workflow 82, 311
- Workflow-Management 87, 311
- Workspace 407
- WORM-Speichermedien 305

Z

- Zertifizierung 34
- Zugriffskontrollen 246
- Zurechenbarkeit 214
- Zutritts- und Zugangskontrollen 246