

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-Serviceerbringungsprozesse	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	Geschäftsfortführungspläne	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