HANSER

Leseprobe

Manuela Reiss, Georg Reiss

Praxisbuch IT-Dokumentation

Vom Betriebshandbuch bis zum Dokumentationsmanagement – die Dokumentation im Griff

ISBN (Buch): 978-3-446-44599-4

ISBN (E-Book): 978-3-446-44812-4

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-44599-4

sowie im Buchhandel.

Inhalt

Vorwort

Nachdem wir bereits vor zwei Jahren unser Buch Praxisbuch IT-Dokumentation überarbeitet und dabei wesentlich erweitert hatten, haben wir uns entschieden, ein weiteres »Major Update« vorzunehmen und die nunmehr 4. Auflage unseres Buchs vorzulegen, die jetzt als 2. Auflage bei Hanser erscheint. Die Triebfeder hierfür waren zum einen die erheblichen Veränderungen und Erweiterungen in den regulatorischen Anforderungen und zum anderen die steigende Bedeutung der Verzahnung bzw. der Schnittstellen zwischen der IT-Organisation und den Business-Einheiten.

Da sind die bereits ergrauten Grundsätze ordnungsgemäßer Speicherbuchführung (GoBS) nach nunmehr 20 Jahren überarbeitet und in 2015 in eine neue Verwaltungsvorschrift, den GoBD, überführt worden. Die bisher schon zentrale Forderung nach einer Verfahrensdokumentation wurde in Ihrer Bedeutung noch verstärkt. Einzuhalten sind die Anforderungen von allen buchführungspflichtigen Unternehmen in Deutschland und das sind die allermeisten. Aber nicht nur im Bereich rechnungslegungsrelevanter IT-Verfahren, sondern insbesondere in Bezug auf die IT-Sicherheit hat es erhebliche Erweiterungen der Anforderungen gegeben. Hervorgerufen werden sie durch das in 2015 veröffentlichte IT-Sicherheitsgesetz in Kombination mit dem ebenfalls 2015 verabschiedeten IT-Sicherheitskatalog gemäß Energiewirtschaftsgesetz (EnWG). In beiden Gesetzen wird explizit (EnWG) bzw. implizit (IT-Sicherheitsgesetz) die anforderungsgerechte Umsetzung der ISO 27001 von Unternehmen gefordert, die den kritischen Infrastrukturen angehören, also u. a. Energieversorgung, Verkehr, Finanzen.

Mit der verpflichtenden Anwendung der ISO 27001[1] geht nicht weniger als ein kompletter Perspektivwechsel von der IT-bezogenen Sicherheit hin zu einer unternehmensweit ausgerichteten Informationssicherheit einher. Diese Norm beschreibt die Implementierung von Informationssicherheitsprozessen im Unternehmen und umfasst die gesamte Organisation von der Managementebene bis zu einzelnen operativen Maßnahmen, wobei die Sicherheit der eingesetzten IT-Systeme einen Teilbereich darstellt. Für eine compliance-gerechte Organisation reicht die Fokussierung auf IT-Sicherheit also nicht mehr aus. Sie wird in die Informationssicherheitsprozesse eingebunden, sozusagen verzahnt.

Das hat Auswirkungen auf die Organisation der IT und auf deren Dokumentation. Eben diese Verzahnung und damit auch die Schnittstellen von IT-Organisation zu den Business-

[1] Im Buch werden der Übersichtlichkeit halber ISO-Normen abgekürzt als ISO *xy* bezeichnet, auch wenn es sich dabei beispielsweise um eine EN ISO oder eine DIN EN ISO handelt.

Einheiten erfahren durch den Perspektivwechsel einen erheblichen Bedeutungsgewinn. Sie sind entsprechend zu organisieren und zu dokumentieren. Besonders deutlich wird das an der Anwendungsdokumentation, die sowohl einen fachlichen Teil als auch einen IT-bezogenen Teil hat. Um eine anforderungsgerechte Anwendungsdokumentation zu erstellen, müssen Fach- und IT-Seite abgestimmt, also verzahnt, zusammenarbeiten. Da die Einführung bzw. die Veränderung von Anwendungen i. d. R. in Projekten organisiert ist, haben wir diesen neuen Schwerpunkt, Anwendungsdokumentation, im Kapitel 5, Dokumentation von IT-Projekten, aufgenommen.

Aber nicht nur innerhalb unseres Praxisbuchs zur IT-Organisation gab es Erweiterungen und neue Schwerpunkte. Aus der Erkenntnis der Notwendigkeit zur Bereitstellung einer einheitlichen und konsistenten Begriffsbildung hat sich für uns das Erfordernis ergeben, diesen notwendigen Begriffsklärungen und-beschreibungen noch mehr Raum zu verschaffen. Da dies im Rahmen des Buchs nur eingeschränkt möglich ist, haben wir einen Blog zum Thema unter der Adresse www.itdoku-kompakt.de veröffentlicht. Hier beschreiben wir Begriffe rund um das Thema IT-Dokumentation, und zwar wesentlich ausführlicher als es im Buch möglich wäre.

Was erwartet Sie in der neuen Auflage?

Bei allen Erweiterungen und neuen Schwerpunkten haben wir die Struktur dieses Buchs nicht verändert.

Um das Buch weiterhin durchgängig und praxistauglich zu gestalten, führen wir Sie Schritt für Schritt durch Ihr Dokumentationsprojekt zum Aufbau bzw. zur Optimierung Ihrer IT-Dokumentation. Als Leitschnur dienen hierbei die folgenden Fragestellungen:

- Warum muss dokumentiert werden?
- Welche Dokumentationsfelder gibt es? Wie kann eine IT-Dokumentation strukturiert werden?
- Was gehört zur Dokumentation für den IT-Betrieb?
- Was sind notwendige Dokumente der Notfalldokumentation?
- Worauf ist bei der IT-Projektdokumentation zu achten?
- Wie können Dokumentationsanforderungen in der Praxis umgesetzt werden?
- Mit welchen Tools kann dokumentiert werden?

Zu einer höheren Praxistauglichkeit trägt auch der in der letzten Auflage entwickelte Strukturierungsansatz bei, der die Dokumentationserfordernisse der IT-Organisationen gemäß ihrer unterschiedlichen Ausprägungen hinsichtlich Prozess- und Serviceorientierung in fünf Stufen abbildet. Wie uns die Erfahrungen aus den vorangegangenen Ausgaben des Praxishandbuchs IT-Dokumentation zeigen, ist es schwierig, aus einem komplexen generischen Modell die für das eigene Unternehmen relevanten Dokumente zu identifizieren.

Was erwartet Sie in den einzelnen Kapiteln?

Unabhängig davon, ob Sie den Aufbau Ihrer IT-Dokumentation oder eine Reorganisation planen: Zu Beginn müssen Sie Ihre Ziele und Anforderungen ermitteln. Diese leiten sich aus gesetzlichen Verpflichtungen, Normen und Standards, aber auch aus wirtschaftlichen und anderen unternehmensstrategischen Entscheidungen ab. Leider wird in der Praxis die Analyse der Ziele und Anforderungen häufig vernachlässigt. Stattdessen wird oft ein Tool angeschafft, ohne aber zu wissen, wohin die Reise eigentlich gehen soll. In **Kapitel 1,**

»Anforderungen an die IT-Dokumentation« möchten wir Sie bei der Beantwortung dieser Fragen unterstützen. Hierbei betrachten wir, welche Dokumentationsanforderungen sich aus gesetzlichen Regelungen und anderen Compliance-Anforderungen ableiten lassen und welche Standards und Zertifizierungen Relevanz für die IT-Dokumentation haben. Außerdem beleuchten wir, welche Anforderungen Prüfer auf Basis der international und national gültigen Prüfungsstandards stellen, da »Revisionssicherheit« und »Compliance« nicht nur Schlagwörter sind, sondern eine immer höhere Bedeutung erlangen.

Im nächsten Schritt möchten wir mit Ihnen das Grundgerüst einer ganzheitlichen Dokumentation »zimmern«. Dazu zeigen wir Ihnen in **Kapitel 2, »Strukturierung einer ganzheitlichen IT-Dokumentation«**, welche Bereiche im Rahmen der IT-Dokumentation zu berücksichtigen sind, und wir werden dabei die IT-Dokumentation auch im Kontext einer unternehmensweiten Dokumentation betrachten.

Nachdem gewissermaßen der »Schrank« für die IT-Dokumentation steht, werden wir mit Ihnen gemeinsam in den daran anschließenden Kapiteln »die Schubladen dieses Schranks füllen«. Hierzu erläutern wir, welche Dokumente im Rahmen der **»Betriebsdokumentation« (Kapitel 3)**, der **»Notfalldokumentation« (Kapitel 4)** und der **»Projektdokumentation« (Kapitel 5)** zu erstellen sind.

Einen Schwerpunkt bildet dabei die **Betriebsdokumentation**. Auf Basis eines Strukturierungsmodells möchten wir Sie dabei unterstützen, eine für Ihre IT-Organisation passende Struktur zu entwickeln und die erforderlichen Dokumente zu ermitteln. Seit der ersten Auflage war es unser Anspruch, einen Ansatz für den Aufbau einer IT-Dokumentation zu bieten, der generisch ist und für jede Unternehmensgröße[2, 3] passt. Die zuvor beschriebenen Erweiterungen in Richtung eines service- und prozessorientierten Ansatzes erfordern aber eine komplexere Struktur. Und diese kann nicht für alle Unternehmen passen, da sich natürlich jede IT-Organisation in einer anderen Situation befindet. Aus diesem Grund haben wir ein Stufenmodell entwickelt, mit dem Sie einfach ermitteln können, wie eine für Ihr Unternehmen passende IT-Dokumentation aussehen kann und was zu dokumentieren ist.

Bis zu diesem Schritt wissen Sie, »Warum« und »Was« es zu dokumentieren gilt. Im anschließenden **Kapitel 6 »Umsetzung in der Praxis«** steht das »Wie« im Mittelpunkt, beispielsweise mit der Frage: Wie schaffe ich es, die Dokumentation aktuell zu halten?

An dieser Stelle werden wir häufig nach Vorlagen für die verschiedenen Dokumente gefragt. Achtung: Dieses Buch versteht sich nicht als eine Sammlung von Vorlagen, mit denen schematisch Dokumente erstellt werden können. Denn unsere jahrelangen Erfahrungen zeigen, dass diese nur eines erzeugen: Dokumente, die nach der Fertigstellung (und der Vorlegung beim Auditor) irgendwo in den Weiten des Dateisystems verschwinden.

Entscheidend ist vielmehr, individuelle und auf die Bedürfnisse des eigenen Unternehmens ausgerichtete Dokumente zu erstellen, diese aktuell zu halten und weiterzuentwickeln. Hierzu bedarf es der Einrichtung eines Dokumentationsmanagements. Ohne ein solches ist es kaum möglich, eine nachhaltige Dokumentation bzw. IT-Dokumentation aufzubauen. Ohne festgelegte Verantwortlichkeiten, Richtlinien und definierte Abläufe wird es nicht ge-

---

[2] Wenn in diesem Buch von Unternehmen die Rede ist, sind damit in gleicher Weise auch andere Organisationen wie Behörden, Körperschaften usw. gemeint.

[3] Wenn bei personellen Bezeichnungen die männliche Form gewählt wurde (z. B. Mitarbeiter, Administrator), so ist damit in gleicher Weise die weibliche Form (Mitarbeiterin, Administratorin) gemeint.

lingen, aus einer unzusammenhängenden Sammlung von Dokumenten eine ganzheitliche Dokumentation aufzubauen. Einen Schwerpunkt des Kapitels zur Umsetzung in der Praxis bilden deshalb die Dokumentationsrichtlinie sowie die erforderlichen Dokumentationsverfahren. Wie wir Ihnen zeigen werden, ist eine solche Richtlinie ein gutes Instrument zur Umsetzung der Dokumentationsziele und Anforderungen.

Aber natürlich ist es hilfreich, bei der Erstellung von Dokumenten auf die eine oder andere Vorlage zurückgreifen zu können. Soweit möglich und sinnvoll, liefern wir Ihnen Beispiele und mögliche Inhalte für zu erstellende Dokumente und verweisen auf hilfreiche Quellen.

Bleibt als letzte Frage offen: Womit, d. h. mit welchen Tools kann dokumentiert werden? Diese werden in **Kapitel 7 »Eine Toolbox für die IT-Dokumentation«** behandelt. Je umfangreicher die Anzahl an Dokumenten und je größer die Komplexität der Abhängigkeiten ist, desto stärker ist das Erfordernis nach einer zentralen IT-gestützten Datenhaltung und Tool-Unterstützung bei der Dokumentation. Auch in dieser Auflage stellen wir Ihnen daher eine Reihe von Tools vor, die Sie bei der Bewältigung der unterschiedlichen Dokumentationsaufgaben unterstützen können. Dabei ist uns klar, dass wir uns hiermit dem Vorwurf einer willkürlichen und nicht objektiven Auswahl aussetzen.

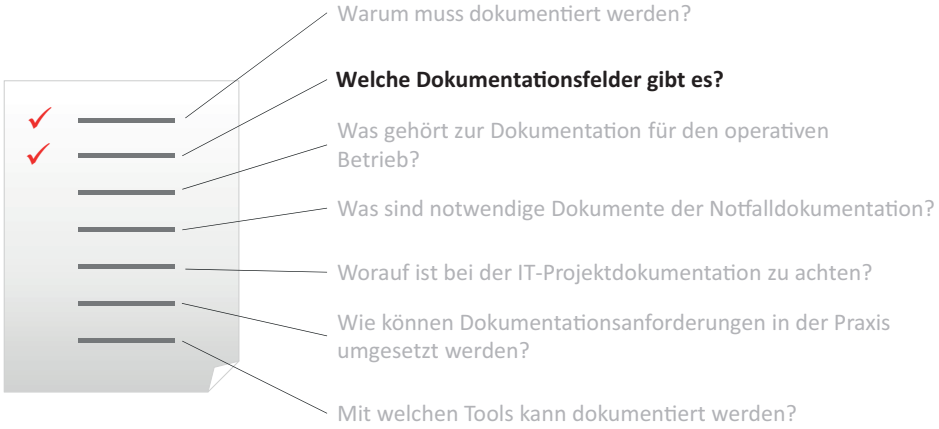
Wir haben jedoch in keiner Weise den Anspruch, Ihnen den Sieger eines fundierten Vergleichstests zu präsentieren, und wir behaupten auch nicht, das beste oder einzig mögliche Tool vorzustellen. Wir möchten Ihnen lediglich exemplarisch anhand von durch uns als nützlich eingestuften Tools zeigen, wie Anwendungen Sie bei der Bewältigung der verschiedenen Dokumentationsaufgaben unterstützen können, und wir möchten Ihnen insbesondere Anregung für die zwingend notwendige Evaluierung bieten. Nicht mehr und nicht weniger.

Wir freuen uns auf Ihr Feedback und auf einen regen Gedankenaustausch, auch zu unserem Blog »itdoku-kompakt«!

Ihre Autoren Manuela und Georg Reiss

info@dokuit.de

2 Strukturierung einer ganzheitlichen IT-Dokumentation



»Wir wollen nun endlich unsere IT-Dokumentation optimieren.« Häufig scheitert dieser gut gemeinte Vorsatz daran, dass man einfach nicht weiß, wo man beginnen soll und was alles zu berücksichtigen ist.

Zwingend erforderlich ist es deshalb, zunächst eine Strukturierung für die eigene Dokumentation zu definieren und auf dieser Basis eine Bestandsanalyse durchzuführen. Dieses Kapitel will dabei unterstützen. Im ersten Teil des Kapitels geht es um die Beantwortung der beiden Fragen: Welche Dokumentationsfelder gibt es? Wie sieht eine sinnvolle Struktur für die IT-Dokumentation aus?

Nachdem damit gewissermaßen der »Schrank« für die IT-Dokumentation steht, werden in den nachfolgenden Kapiteln »die Schubladen dieses Schranks gefüllt« und die einzelnen Bereiche detailliert vorgestellt. Dabei wird eine dieser Schubladen bereits in diesem Kapitel betrachtet. Der zweite Teil behandelt das Thema Rahmendokumente: Was sind Rahmendokumente? Welche sind erforderlich?

In diesem Kapitel finden Sie die folgenden Themenschwerpunkte:

- Services, Prozesse, Systeme – was muss dokumentiert werden?
- Bausteine einer ganzheitlichen IT-Dokumentation
- Rahmendokumente
- Abgrenzung zur technischen Dokumentation

2.1 Services, Prozesse, Systeme – was muss dokumentiert werden?

Lange Zeit war die vorherrschende Organisationsform von Unternehmen funktionsorientiert. Eine funktionsorientierte Ausrichtung ist geprägt durch vertikale Hierarchien, eine entsprechende aufbauorganisatorische Struktur und eine starke Trennung zwischen Fach- und Ressourcenverantwortung. Das heißt, jede einzelne Organisationseinheit ist nur für jeweils den eigenen Schritt in dieser Kette zuständig.

Doch immer mehr Unternehmen erkennen, dass ein ausgeprägter Servicegedanke mit einer gut funktionierenden Kundenbeziehung entscheidend für den Geschäftserfolg ist. Serviceorientierung, Prozessorientierung und Kundenorientierung stehen daher zunehmend im Fokus der Unternehmen. Und diese neue Ausrichtung erfordert veränderte Organisationsstrukturen, die auch die IT-Organisationen betreffen. Diese stehen immer häufiger in der Pflicht, sich als interne Service-Provider aufzustellen, die ihren internen Kunden vertraglich geregelte Dienstleistungen mit definierten SLAs anbieten. Gleichzeitig drängen in immer kürzeren Abständen neue Technologien in den Markt, die von der IT 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. So reicht es nicht mehr, allein die vorhandenen Systeme zu dokumentieren.

2.1.1 Komponenten eines serviceorientierten IT-Betriebs

Den beschriebenen Anforderungen entsprechend, muss eine ganzheitliche IT-Dokumentation die in Bild 2.1 gezeigten Komponenten berücksichtigen. Welche Komponenten davon im Einzelfall zu berücksichtigen sind, hängt auch vom jeweiligen Grad der Service- und Prozessorientierung der IT-Organisation ab.

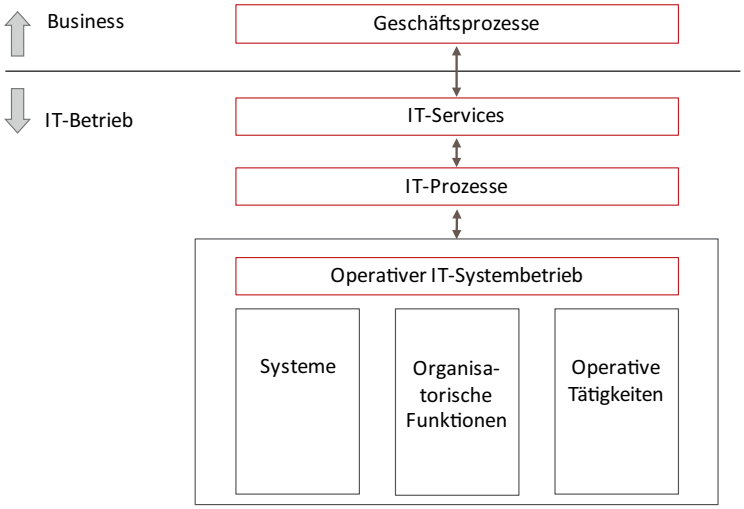


Bild 2.1 Bereiche eines serviceorientierten IT-Betriebs und deren Abhängigkeiten

Ein *Service* ist ein Mittel zur Generierung von Nutzen für den Kunden. Er liefert vereinbarte Ergebnisse, ohne dass die Kunden für die servicespezifischen Kosten und Risiken Verantwortung tragen müssen. Und ein *IT-Service* ist gemäß Definition des *IT Service Management Forum (itSMF) Arbeitskreis Publikation ITIL® Version 3 Translation Project »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)

Ein *Prozess* ist hierbei als eine Kette aufeinander aufbauender, funktionsübergreifender Arbeitsschritte bzw. Aktivitäten zu betrachten, durch die ein klar definierter Input in einen definierten (materiellen oder immateriellen) Output umgewandelt wird. Er beginnt mit einem definierten Auslöser und endet mit einem definierten Ergebnis. Wichtige Punkte sind hierbei:

- Prozesse gehen über hierarchische Organisationseinheiten hinweg,
- Prozesse überschreiten häufig Organisationsgrenzen,
- Prozesse unterliegen einer besonderen Bewertung auf Basis von Schlüsselindikatoren (KPI).

Bei einer prozessorientiert agierenden IT-Organisation stehen die Geschäftsprozesse im Mittelpunkt der betrieblichen IT-Organisation und der Betrieb erfolgt auf Basis definierter Prozesse und standardisierter Verfahren. 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. Die Mitarbeiter werden dabei bestimmten Prozessteams zugeordnet, die einen Prozess von Anfang bis Ende betreuen. Dadurch entstehen flache Hierarchien mit kurzen Informationswegen. Im Idealfall werden die Selbstorganisationsfähigkeiten der Teams gestärkt.

Beispiel: Funktionsorientierung versus Prozessorientierung

Bei einer an den Funktionen orientierten Organisationsstruktur gibt es ein Team, das für die Client-Rechner und jeweils ein Team, das für Active Directory bzw. das Mail-System zuständig ist. Außerdem gibt es noch ein Team, das den Benutzersupport verantwortet und auch Serviceanfragen abwickelt. Kommt nun ein neuer Mitarbeiter in das Unternehmen, werden in vollkommen separaten Arbeitsschritten durch unterschiedliche Personen mit dementsprechend eingeschränkten Befugnissen ein neues Benutzerkonto, ein Postfach und ein Arbeitsplatzrechner für den neuen Mitarbeiter eingerichtet. Es ist leicht vorstellbar, dass es hierbei an den Schnittstellen zu Kommunikationsproblemen und Schwierigkeiten bei der Abgrenzung der Verantwortung kommen kann.

Beim prozessorientierten Ansatz hingegen gibt es einen Prozess »Neuer Mitarbeiter«. Der Mitarbeiter benötigt einen Arbeitsplatz mit Tisch und Stuhl, einen Rechner, ein Benutzerkonto, ein Postfach und diverse Zugriffe. Alle diese Aufgaben werden als eine Abfolge von Aktivitäten betrachtet, die von einer (einzigen) Person verantwortet und koordiniert werden. Alle Informationen bleiben damit in einer Hand und die Abstimmungsprozesse werden reduziert und gesteuert, da die Schnittstellen und die jeweiligen Inputs und Outputs definiert sind. ■

Ein *Geschäftsprozess*, auch *Unternehmensprozess* genannt, ist ein Prozess, der am Unternehmenszweck ausgerichtet ist und zum Erfolg eines Unternehmens beiträgt. Typischerweise werden die Geschäftsprozesse eines Unternehmens in drei Gruppen unterteilt:

- Der wertschöpfende Betriebsablauf eines Unternehmens besteht aus *Kernprozessen* (auch als *Wertschöpfungsprozesse* oder *Primäre Geschäftsprozesse* bezeichnet). Durch diese Prozesse wird der Mehrwert bzw. die Wertsteigerung des Unternehmens geschaffen. Beispiele hierfür sind Produktionsprozesse, Dienstleistungsprozesse und Vertriebsprozesse.
- Daneben gibt es sogenannte *Unterstützungsprozesse* (auch als *Supportprozesse* oder *Sekundäre Geschäftsprozesse* bezeichnet). Unterstützungsprozesse stellen Ressourcen und Services zur Verfügung und sind darauf ausgerichtet, die Kernprozesse des Unternehmens zu unterstützen. Diese Prozesse erzeugen keinen direkten Kundennutzen. Zu den Unterstützungsprozessen zählen beispielsweise das interne und externe Rechnungswesen sowie das Personalwesen und auch die Informationstechnologie.
- *Managementprozesse* (auch als *Steuerungsprozesse* bezeichnet) dienen der Steuerung des Unternehmens und sind für die Verbesserung und Steuerung der Wertschöpfungsprozesse und Unterstützungsprozesse zuständig. Sie ermöglichen es, die Unternehmensziele zu verfolgen, die damit verbundenen Risiken zu definieren und zu bewerten sowie die Zielerreichung zu überwachen. Zu den Managementprozessen zählen u. a. Prozessoptimierungsprozesse, Innovationsprozesse, Strategieentwicklungsprozesse, aber auch Qualitätsmanagement, Risikomanagementprozesse und nicht zuletzt Überwachungsprozesse.

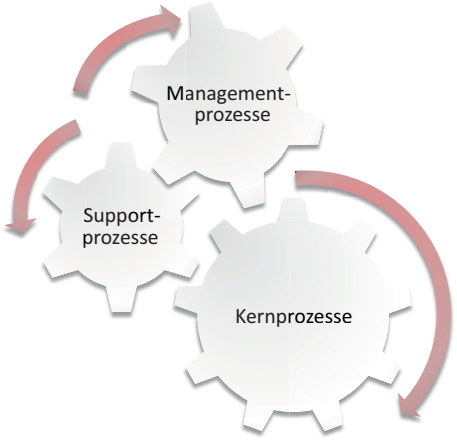


Bild 2.2
Die Kernprozesse werden von den Supportprozessen unterstützt und durch Managementprozesse gesteuert.

IT-Prozesse können auch Kernprozesse sein

IT-Prozesse werden allgemein den Unterstützungsprozessen zugeordnet. Bei einem Softwarehersteller, dessen Kerngeschäft die Entwicklung und Vermarktung von Softwareprodukten ist, gehören Softwareentwicklungsprozesse natürlich zu den Kernprozessen, die wiederum durch IT-interne Supportprozesse unterstützt werden.

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 völlig. 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-Servicemanagement 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)

Der Begriff *IT-System* ist keineswegs einheitlich definiert. So sind gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI) *»IT-Systeme technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.«* (BSI Grundschutz-Glossar)

Im Duden Informatik hingegen wird der Systembegriff deutlich weiter gefasst und so auch im Buch verwendet: *»System: In der Informatik versteht man hierunter die Zusammenfassung mehrerer Komponenten zu einer als Ganzes aufzufassenden Einheit. Die Komponenten können von gleicher Art (homogene Systeme, z. B. Programme) oder sehr unterschiedlich sein (z. B. die Zusammenfassung von Hardware- und Softwaresystemen zu einem System. […] Ein System löst oder bearbeitet in der Regel ein definiertes Bündel von Aufgaben.«* (Duden, 1993)

Im vorliegenden Buch wird der Begriff IT-System im Sinne des BSI verwendet. Zum einen erleichtert dieser Ansatz die Dokumentation und zum anderen bietet er den Vorteil, dass das BSI in den IT-Grundschutzkatalogen jeweils neben einer Kurzbeschreibung der betrach-

teten Komponenten einen Überblick über die Gefährdungslage sowie Maßnahmenempfehlungen liefert, so dass auch Unternehmen, die keine BSI-Grundschutzausrichtung verfolgen, dort wertvolle Informationen finden.

2.1.2 Dokumente und Aufzeichnungen

Die IT-Organisation muss sicherstellen, dass das Service-Management-System nachvollziehbar ist und bleibt. Dazu sind *Dokumente* und *Aufzeichnungsdokumente* (in der Regel als *Aufzeichnungen* bezeichnet) notwendig, nicht nur aus Compliance-Gründen (siehe Kapitel 1), 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, Richtliniendokumente, 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 Revisionstände. Typischerweise zählen Systemprotokolle, Auswertungen (Reports, Analysen, Statistiken), Protokolle (Testprotokolle, Abnahmeprotokolle u. a.), ausgefüllte Formulare und Checklisten zu den Aufzeichnungen.

Wichtig ist, dass Dokumente und Aufzeichnungen unterschiedlich zu verwalten sind. Hier liefert die Qualitätsmanagementnorm DIN EN ISO 9001:2008 mit ihrer Forderung zur Einrichtung zweier Verfahren zur Lenkung von Dokumenten und zur Lenkung von Aufzeichnungen wertvolle Hinweise (Informationen zu Verfahren und Verfahrensbeschreibungen finden Sie in *Abschnitt 3.8.15*).

Die beiden Verfahren sind wie folgt definiert:

»4.2.3 Lenkung von Dokumenten

Die vom Qualitätsmanagementsystem geforderten Dokumente müssen gelenkt werden. Aufzeichnungen stellen einen besonderen Dokumententyp dar und müssen nach den in 4.2.4 genannten Anforderungen gelenkt werden.

Ein dokumentiertes Verfahren zur Festlegung der erforderlichen Lenkungsmaßnahmen muss eingeführt werden, um

a) Dokumente bezüglich ihrer Angemessenheit vor ihrer Herausgabe zu genehmigen,

b) Dokumente zu bewerten, sie bei Bedarf zu aktualisieren und erneut zu genehmigen,

c) sicherzustellen, dass Änderungen und der aktuelle Überarbeitungsstatus von Dokumenten gekennzeichnet werden,

d) sicherzustellen, dass gültige Fassungen zutreffender Dokumente an den jeweiligen Einsatzorten verfügbar sind,

e) sicherzustellen, dass Dokumente lesbar und leicht erkennbar bleiben,

f) sicherzustellen, dass Dokumente externer Herkunft, die die Organisation als notwendig für die Planung und den Betrieb des Qualitätsmanagementsystems eingestuft hat, gekennzeichnet werden und ihre Verteilung gelenkt wird, und

g) die unbeabsichtigte Verwendung veralteter Dokumente zu verhindern und diese in geeigneter Weise zu kennzeichnen, falls sie aus irgendeinem Grund aufbewahrt werden.

»4.2.4 Lenkung von Aufzeichnungen

Aufzeichnungen, die erstellt werden, um Nachweise der Konformität mit den Anforderungen und des wirksamen Funktionierens des Qualitätsmanagementsystems bereitzustellen, müssen gelenkt werden.

Die Organisation muss ein dokumentiertes Verfahren erstellen, um die Lenkungsmaßnahmen festzulegen, die für die Kennzeichnung, die Aufbewahrung, den Schutz, die Wiederauffindbarkeit und die Aufbewahrungsfrist von Aufzeichnungen sowie die Verfügung über Aufzeichnungen erforderlich sind.

Aufzeichnungen müssen lesbar, leicht erkennbar und wieder auffindbar bleiben.« (ISO 9001, 2008)

2.2 Bausteine einer ganzheitlichen IT-Dokumentation

Wie in *Kapitel 1* ausgeführt, ist in den vergangenen Jahren die Anzahl an gesetzlichen Anforderungen, Richtlinien und branchenspezifischen Regelungen deutlich angestiegen. Eine gut strukturierte, vollständige und aktuelle Dokumentation ist die Basis für die Umsetzung aller Compliance-Anforderungen und dient darüber hinaus als Nachweis für die Umsetzung von Maßnahmen, beispielsweise zur Sicherstellung eines angemessenen internen Kontrollsystems (IKS).

Die Schwierigkeit beim Aufbau bzw. bei der Strukturierung der IT-Dokumentation besteht aber darin, dass diese sehr unterschiedlichen Sichten von verschiedenen Benutzern und damit unterschiedlichen Anforderungen Rechnung tragen muss. Und Auditoren und Prüfer haben zwangsläufig eine andere Sicht auf die Dokumentation als die Mitarbeiter des Service Desk.

Der im Folgenden vorgeschlagene und im Buch verwendete Aufbau zeigt daher lediglich eine mögliche logische Struktur, nicht jedoch die physische Strukturierung im Filesystem oder in anderen Anwendungen. In der Praxis hat es sich bewährt, mit einer solchen Strukturierung zu arbeiten und diese als Basis für den Aufbau einer IT-Dokumentation zu verwenden. Ob die Umsetzung dann in Form von Ordnern oder beispielsweise als Metadaten im Dokumentenmanagementsystem erfolgt, spielt für die Strukturierung keine Rolle und ist unternehmensspezifisch festzulegen.

Ausgangspunkt der hier vorgestellten Struktur einer ganzheitlichen Dokumentation für den IT-Bereich sind die Geschäftsprozesse. In einer solchen Unternehmensdokumentation ist die IT-Dokumentation ein Teilbereich, der aber diverse Schnittstellen zu anderen Bereichen aufweist.

Einordnung in die Unternehmensdokumentation

Bild 2.3 zeigt die mögliche Struktur einer unternehmensweiten und an Geschäftsprozessen ausgerichteten Dokumentation. Entsprechend der im vorstehenden Kapitel dargestellten Unterscheidung in die Kernprozesse, Supportprozesse und Managementprozesse können die nachstehenden Bereiche unterschieden werden:

- Dokumentation der Kernprozesse.
- Dokumentation der Unterstützungsprozesse. Hierzu zählt auch die IT-Dokumentation.
- Dokumentation der Managementprozesse. Beispielsweise können die Dokumente des Qualitätsmanagements, des Risikomanagements und auch des unternehmensweiten Sicherheits- und Notfallmanagements diesem Bereich zugeordnet werden.

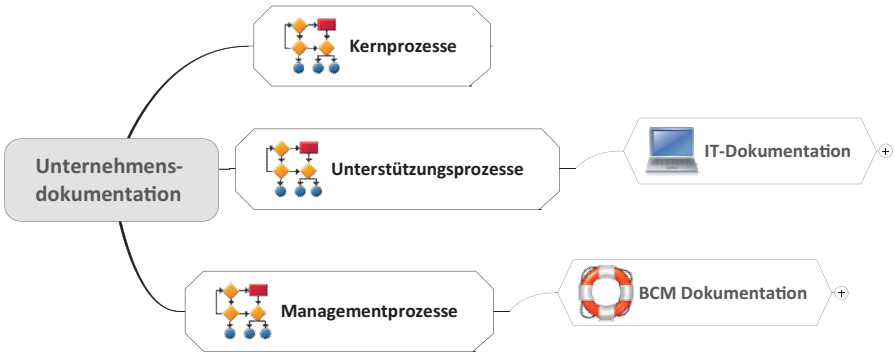


Bild 2.3 Die IT-Dokumentation als Teil der Unternehmensdokumentation

Die dargestellte Struktur bietet den Vorteil, dass zusätzliche unternehmensspezifische Dokumentationsbereiche wie beispielsweise das Qualitätsmanagement problemlos integriert werden können. Im Fokus des Buchs steht die IT-Dokumentation. Deshalb wird auf eine weitergehende Betrachtung der Unternehmensdokumentation verzichtet. Sofern sinnvoll, wird aber in den nachfolgenden Kapiteln auf die entsprechenden Schnittstellendokumente der Unternehmensdokumentation hingewiesen.

Aufbau der IT-Dokumentation

Bei der Strukturierung der IT-Dokumentation hat sich wiederum in der Praxis eine Aufteilung in vier Dokumentationsbereiche bewährt:

- **Betriebsdokumentation:** Der IT-Betrieb umfasst neben dem operativen Systembetrieb und den damit verbundenen operativen Aufgaben zur Steuerung und zur Optimierung der Systeme alle Aufgaben, die zur Erbringung von IT-Services erforderlich sind. Dies beinhaltet u. a. alle Dokumente, die zur Sicherstellung des laufenden Betriebs, zur Instandhaltung und zur Fehlerbehebung benötigt werden.

- **Notfalldokumentation:** Das unternehmensweite Notfallmanagement beinhaltet alle Aufgaben der Notfallvorsorge und der Notfallbewältigung und das IT-Notfallmanagement ist ein Teil davon. Die IT-Notfalldokumentation muss daher Teil einer übergeordneten Notfalldokumentation sein. Als solche muss sie vor allem sicherstellen, dass die kritischen IT-Services auch in Notfällen verfügbar sind bzw. gemacht werden können.
- **Projektdokumentation:** Dieser Bereich beinhaltet alle Dokumente, die im Rahmen von Projekten erstellt werden und der Entwicklung und der Einführung neuer oder geänderter IT-Systeme und -Verfahren dienen.
- **Rahmendokumente:** Rahmendokumente sind vor allem strategische Dokumente mit allgemeinen Vorgaben und Normierungen, sofern diese nicht auf Unternehmensebene geregelt sind. Aber auch die Dokumente des IT-Managements können den Rahmendokumenten zugeordnet werden.

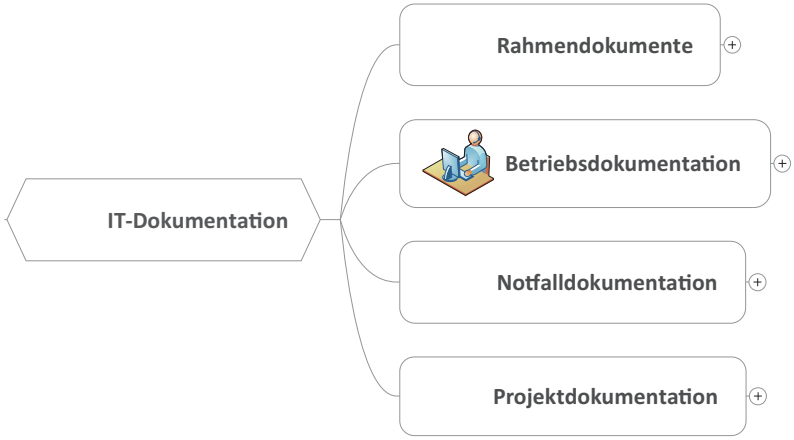


Bild 2.4 Die vier Dokumentationsbereiche der IT-Dokumentation

Ausführliche Vorstellung der Bereiche in gesonderten Kapiteln

Die folgenden Ausführungen stellen die drei Bereiche *Betriebsdokumentation*, *Notfalldokumentation* und *Projektdokumentation* im Überblick vor und bieten damit eine kurze Einführung in das jeweilige Thema. Zusätzlich werden die drei Bereiche jeweils gesondert in einem Kapitel behandelt. Die Rahmendokumente hingegen werden in diesem Kapitel in *Abschnitt 2.3* ausführlich vorgestellt.

2.2.1 Betriebsdokumentation

In der Praxis besteht die Herausforderung vor allem darin, die vielen verschiedenen Dokumente, die für den IT-Betrieb benötigt werden bzw. während des Betriebs erstellt werden, zu strukturieren und sicherzustellen, dass alle Dokumente und Informationen jeweils aktuell für die unterschiedlichen Einsatzbereiche zur Verfügung stehen.

Die Strukturierung der Dokumente ist deshalb der erste und wichtigste Schritt auf dem Weg zu einer nachhaltigen Dokumentation, die nicht nur die Compliance-Anforderungen erfüllt, sondern auch die betrieblichen Abläufe unterstützt. Das in *Abschnitt 3.1* vorgestellte Strukturierungsmodell für die IT-Betriebsdokumentation kann dabei unterstützen. Dieses unterscheidet auf der obersten Ebene eine Dokumentation für die folgenden Bereiche:

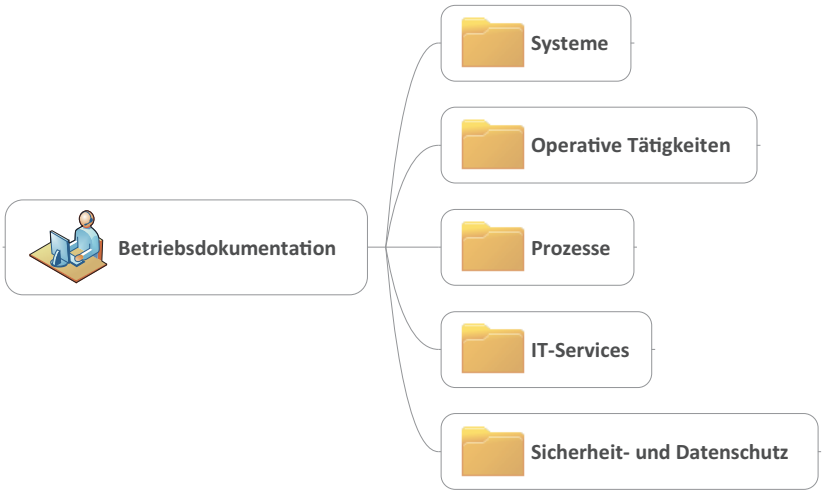


Bild 2.5 Bereiche der IT-Betriebsdokumentation

- **Systeme:** Systeme bilden die Basis für die Bereitstellung von IT-Dienstleistungen, unabhängig davon, welchen Reifegrad eine IT-Organisation hinsichtlich Service- und Prozessorientierung erreicht hat. Die Einrichtung und Pflege einer Systemdokumentation als Bestandteil der IT-Betriebsdokumentation sind daher zwingend erforderlich. Diese muss die eingesetzten Hardwarekomponenten (Server- und Clientsysteme) genauso beinhalten wie Beschreibungen des Verzeichnisdienstes, der Server- und Netzwerkdienste, der eingesetzten Anwendungen sowie der Netzwerkkomponenten. Zusätzlich gehören diverse Pläne, wie beispielsweise Netzwerkpläne, zur Systemdokumentation.
- **Operative Tätigkeiten:** Dieser Teil der IT-Dokumentation beschreibt die Abläufe des täglichen operativen IT-Betriebs. Sind die operativen Tätigkeiten gut und nachvollziehbar dokumentiert, erleichtern sie nicht nur die Routinearbeiten. Außerdem können personelle Ausfälle leichter kompensiert werden und neue Mitarbeiter sich schneller einarbeiten. Zudem bleibt wertvolles Know-how erhalten, wenn Mitarbeiter das Unternehmen verlassen. 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 *Betriebshandbüchern* dokumentiert. Betriebshandbücher beschreiben »wer, was, wann, wie, wie oft« tun muss, um den operativen IT-Betrieb einschließlich der erforderlichen Kontroll- und Wartungsarbeiten sicherzustellen, d. h. die operativen Tätigkeiten. Sinnvollerweise werden die Betriebshandbücher durch Arbeitsanleitungen bzw. Arbeitsanweisungen und Ablaufbeschreibungen ergänzt. 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 Änderungen umfassen.

- **Prozesse:** 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. Im Gegensatz zu den operativen Tätigkeiten beschreiben Prozesse die operative Ebene nicht detailliert. Im Fokus stehen vielmehr betriebswirtschaftliche Faktoren wie Kosten und Erlöse. Kennzahlen sind daher eine wichtige Prozesseigenschaft.
- **IT-Services:** In dieser Kategorie wird die Ausprägung des IT-Servicemanagements (ITSM) betrachtet. Die Aufgabe von IT-Servicemanagement ist es, 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 Kunden bieten. Die Ausprägung von IT-Servicemanagement reicht von einzelnen definierten IT-Services über einen definierten Servicekatalog mit zusammenhängenden und aufeinander aufbauenden Services bis hin zu gelebten Service-Lebenszyklus-Prozessen. Dem steht eine IT-Dokumentation gegenüber, die von einzelnen Servicebeschreibungen bis hin zur Abbildung der Services in Form von Configuration Items in entsprechenden Datenbanken reicht.
- **Sicherheit und Datenschutz:** Unabhängig von der Größe oder dem aktuellen Grad der Prozess- und Serviceorientierung unterliegt jede IT-Organisation Anforderungen an die Informationssicherheit und den Datenschutz und muss diese entsprechend nachweisen. Die zunehmende IT-Durchdringung macht es erforderlich, dass die IT einen großen Beitrag zur Informationssicherheit des Unternehmens leisten muss. Sie hat zu gewährleisten, dass erforderliche Daten tatsächlich verfügbar sind, schützenswerte Daten vertraulich bleiben und ein Unternehmen mit unverfälschten und zuverlässigen Daten arbeiten kann.

Individuelle Ausprägungen bestimmen die Struktur der Dokumentation

Jedes Unternehmen und jede IT-Organisation sind anders. Die Dokumentation muss daher ebenfalls individuell betrachtet werden und an die eigenen Anforderungen angepasst werden. Eine IT-Organisation, die serviceorientiert aufgestellt ist, benötigt auch die zugehörige Servicemanagement-Dokumentation. IT-Organisationen, deren Arbeitsweise hingegen überwiegend an den Funktionen und Systemen ausgerichtet ist, können darauf nachvollziehbarerweise verzichten. Das vorliegende Buch kann Ihnen natürlich nur einen generischen Ansatz liefern.

Um Sie bei der Adaption an Ihre individuelle Situation bestmöglich zu unterstützen, wurde für die Betriebsdokumentation ein fünfstufiges Strukturierungsmodell entwickelt, bei dem jede Stufe die komplette IT-Betriebsdokumentation für die beschriebene Stufe abbildet. Nachdem Sie anhand verschiedener Aspekte hinsichtlich Prozess- und Serviceorientierung des IT-Betriebs die für Sie passende Stufe ermittelt haben, finden Sie in einem gesonderten Abschnitt die für Ihre Organisation geeignete Struktur der Betriebsdokumentation sowie die erforderlichen Inhalte.

2.2.2 Notfalldokumentation

Aus einer Reihe der in *Kapitel 1* beschriebenen Anforderungen ergibt sich die Verpflichtung zur Einführung eines effektiven unternehmensweiten Notfallmanagements. Dabei herrscht noch immer in vielen Unternehmen der Irrglaube, dass mit der einmaligen Erstellung eines IT-Notfallhandbuchs, das aufzeigt, wie die Systeme im Notfall wiederherzustellen sind, alles für den Notfall getan ist. Doch nicht die Wiederherstellung der Systeme steht bei einem Notfall im Vordergrund, sondern die Wiederherstellung der Geschäftsprozesse, wie das nachfolgende Beispiel verdeutlicht.

Beispiel: IT-Notfallmanagement als Teil von BCM

Um den Fortbestand des Unternehmens im Notfall zu sichern, fordern gesetzliche Regelungen die Einführung eines unternehmensweiten Notfallmanagements. Ziel eines solchen Notfallmanagements *(Business Continuity Management – BCM)* ist die Aufrechterhaltung bzw. die Wiederaufnahme der wichtigen Geschäftsprozesse im Notfall.

Wird beispielsweise das Hauptgebäude eines Unternehmens durch einen Brand vernichtet, muss das Hauptaugenmerk darauf liegen, für die kritischen Geschäftsprozesse so schnell wie möglich einen Notbetrieb einzurichten. Idealerweise steht hierfür ein Ausweichstandort zur Verfügung. Zum Notbetrieb gehört in der Regel, abhängig vom Unternehmenszweck, in mehr oder weniger großem Umfang auch die Bereitstellung von IT-Systemen. Da hierbei ausschließlich die für das Überleben des Unternehmens erforderlichen Kernprozesse betrachtet werden, sind im Rahmen des Notfallmanagements IT-seitig lediglich die Systeme zu identifizieren, die für eine Aufrechterhaltung dieser Prozesse bzw. für den Notbetrieb auch tatsächlich erforderlich sind. Die Dokumentation dieser IT-Komponenten einschließlich Wiederherstellungsplänen und eine Beschreibung des Wiederanlaufs der IT-Systeme bei Rückkehr in den Normalbetrieb sollten daher Bestandteil eines übergeordneten Notfallplans sein bzw. diesen ergänzen.

Dass sich hinter dem Begriff Notfallmanagement außerdem ein komplexer Prozess verbirgt, wird ebenfalls gerne übersehen. Diesen Prozess beschreibt u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) im *Standard 100-4 Notfallmanagement*, der im Februar 2009 in der finalen Version veröffentlicht wurde. Demzufolge muss der Notfallmanagementprozess sowohl die Notfallvorsorge, die Notfallbewältigung wie auch die Notfallnachsorge umfassen und besteht aus den folgenden Phasen:

- Initiierung eines Notfallprozesses und Erstellung eines Notfallvorsorgekonzepts,
- Erstellung eines Notfallhandbuchs zur Notfallbewältigung,
- Planung (Dokumentation) und Durchführung von Übungen und Tests,
- kontinuierliche Verbesserung des Notfallprozesses.

Dabei genügt es nicht, »Standardnotfälle« wie Brand- oder Wasserschäden in einem klassischen Notfallhandbuch einfach nur zu beschreiben. Vielmehr muss das Notfallhandbuch

alle Informationen enthalten, um im Notfall die erforderlichen Maßnahmen zur Wiederaufnahme des wegen des Notfalls unterbrochenen Betriebs durchführen zu können. Außerdem muss es u. a. Beschreibungen der im Notfall auszuführenden Prozesse enthalten, Melde- und Eskalationswege festlegen und Wiederanlaufpläne und Ausweichprozesse für den Notbetrieb beschreiben. Wichtig ist dabei, dass es trotz der umfangreichen Anforderungen und der notwendigen Komplexität einfache und vollständige Handlungsanweisungen bietet. Und tritt ein Notfall ein, ist die Aufregung meist groß und die Gefahr, die Situation durch fehlerhaftes Verhalten zu verschlimmern, darf nicht unterschätzt werden. Um in einer Notfallsituation handlungsfähig zu bleiben, muss jeder wissen, was zu tun ist. Das aber ist nur möglich, wenn die Inhalte der Notfallpläne regelmäßig getestet und trainiert werden. In den meisten Unternehmen werden zwar Notfallhandbücher bzw. Notfallpläne erstellt, aber entweder gar nicht oder nur einmal getestet bzw. geübt. Viele dieser Pläne versagen dann beim ersten umfassenden Test oder schlimmstenfalls im konkreten Notfall. Aufgrund der Bedeutung und der weitreichenden Konsequenzen muss der Notfallmanagementprozess von der obersten Leitungsebene initiiert, gesteuert und kontrolliert werden.

Wie die Ausführungen zeigen, ist die IT-Notfalldokumentation zwingend als Bestandteil der Notfalldokumentation für das Unternehmen zu behandeln. Auch aus diesem Grund wird sie im Buch als eigenständiger Bereich und von der Betriebsdokumentation getrennt behandelt. Außerdem unterliegt das Management eines Notfalls anderen Abläufen – mit vom Betrieb abweichenden Regelungen.

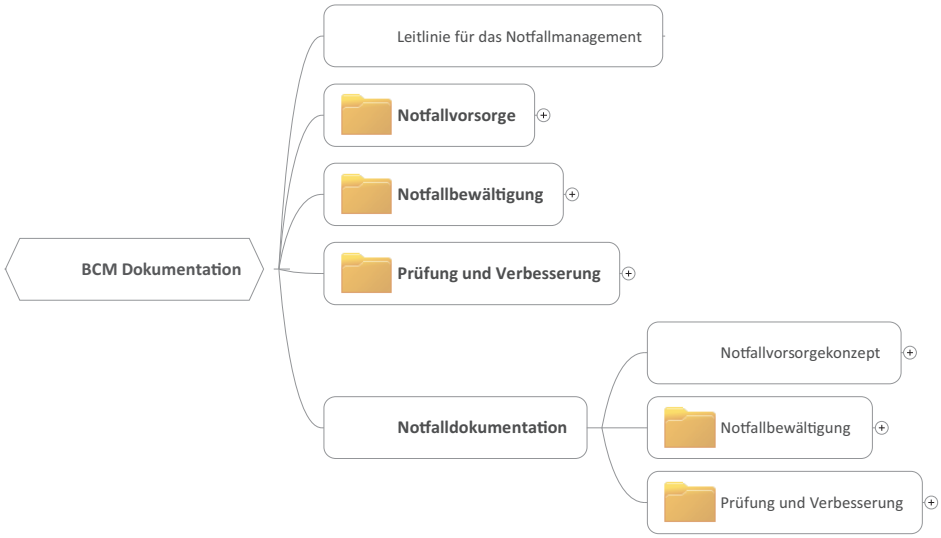


Bild 2.6 IT-Notfallmanagement muss Teil eines unternehmensweiten Notfallmanagements sein.

Gesondertes Kapitel zur Notfalldokumentation

Ausführliche Erläuterungen zu den hier angesprochenen Themen und Anleitungen zur Erstellung der erforderlichen Notfalldokumente finden Sie in *Kapitel 4.*

2.2.3 Projektdokumentation

Im Bereich der IT spielen Änderungsprozesse eine wesentliche Rolle, denn nur wenige Branchen sind wohl derartig häufig Änderungen und Anpassungen unterworfen wie die IT. Dabei können die Auslöser von Änderungen sehr unterschiedlicher Natur sein:

- gesetzliche Anforderungen,
- organisatorische Anforderungen (beispielsweise organisatorische Umstrukturierungen),
- technische Anforderungen,
- Anforderungen, die sich aus Optimierungsprozessen ergeben.

Änderungsaufgaben können sowohl innerhalb des IT-Regelbetriebs erfolgen als auch im Rahmen von Projekten. Insbesondere größere Veränderungen, die eine gesonderte Organisation und deshalb zusätzliche Ressourcen erfordern, werden meist als Projekt durchgeführt. Einen weiteren eigenständigen Baustein der IT-Dokumentation bildet daher die IT-Projektdokumentation.

Wichtiger Dokumentationsbereich: Software- bzw. Systementwicklung

Eine besondere Rolle spielt in diesem Zusammenhang der Bereich der *Software- bzw. Systementwicklung*. In größeren Unternehmen gibt es hierfür häufig einen eigenen Organisationsbereich, der für die Durchführung von Entwicklungsprojekten verantwortlich ist. Auf der anderen Seite handelt es sich um eine Querschnittsaufgabe, in die viele Organisationsbereiche auch aus Sicht der Dokumentation einbezogen sind. So muss der Fachbereich beispielsweise die Vorgaben dokumentieren und der IT-Betrieb zeichnet für die Betriebsdokumentation verantwortlich.

In *Abschnitt 5.3* befassen wir uns ausführlich mit dem Thema *Anwendungsdokumentation*. Wichtig ist uns hierbei eine ganzheitliche Betrachtung ausgehend von der Entwicklung, über die Bereitstellung durch die IT und die Nutzung der Applikation durch den Fachbereich.

Bei der Frage nach einer angemessenen Projektdokumentation stößt man zuerst auf die Überlegung: Was ist überhaupt ein Projekt bzw. wodurch ist ein Projekt definiert? Und diese Frage ist in der Tat nicht so einfach zu beantworten, wie sie sich anhört. Einen guten Ansatz zur Projektdefinition liefert die DIN 69901-5:2009. Demzufolge ist ein Projekt ein *»Vorhaben, das im Wesentlichen durch die Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist«* (DIN 69901, 2009) und sich durch folgende Kriterien auszeichnet:

- Zielvorgaben,
- zeitliche, finanzielle, personelle oder andere Begrenzungen,
- projektspezifische Organisation.

Die *Deutsche Gesellschaft für Projektmanagement e. V. (GPM)* erweitert diese Definition um den Aspekt der Arbeitsteilung und definiert Projekte als arbeitsteilige Prozesse. (Heinz Schelle, 2008)

DIN 69901 Projektmanagement – Projektmanagementsysteme und ISO 21500

Die DIN 69901 »Projektmanagement – Projektmanagementsysteme« ist im Januar 2009 erschienen. Hervorgegangen ist sie aus diversen Vorgängernormen. So wurden die aus der Netzplantechnik entstandenen und mehrmals ergänzten bisherigen Normen DIN 69901, DIN 69902, DIN 69903, DIN 69904 und DIN 69905 der Projektwirtschaft in den Teilen der DIN 69901 zusammengefasst, neu strukturiert, durchgängig aktualisiert und um wesentliche Teile ergänzt. Im Mittelpunkt der neuen fünfteiligen DIN 69901 unter dem Haupttitel *Projektmanagement – Projektmanagementsysteme* steht ein Modell der Prozesse im Projektmanagementsystem. Neu hinzugekommen ist außerdem ein Datenmodell. Wichtig ist aber auch *Teil 5 – Begriffe*. Dieser Normenteil fasst die bisher auf mehrere Normen verteilten Begriffe zusammen. Dabei wurde die Zahl der genormten Begriffe stark reduziert.

Als weiterer Standard steht seit 2012 mit der ISO 21500 »Guidance on Project Management« eine internationale Norm für das Projektmanagement zur Verfügung. Die Norm bietet neben Begriffen und Konzepten für das Projektmanagement vor allem ein durchgängiges Prozessmodell, das im Wesentlichen auf dem amerikanischen PMBOK-Guide und der deutschen Norm DIN 69901-2:2009 basiert. Die ISO 21500 will nationale Normen und Standards ergänzen und zu einer internationalen Harmonisierung beitragen. Unternehmen können die Norm als Anleitung für ihr Projektmanagement-Prozessmodell verwenden oder als Basis für die Abwicklung von Projekten mit internationalen Partnern.

Bei IT-Projekten handelt es sich demzufolge um zielgerichtete sowie zeitlich, personell und sachlich abgegrenzte IT-Vorhaben. Sie beinhalten die Konzeption, die Entwicklung, die Einführung bzw. wesentliche Änderungen von IT-Systemen und IT-Verfahren. Damit haben IT-Projekte die Erweiterung bzw. den Umbau des IT-Betriebs zur Folge. Die Abgrenzung eines Projekts zum Betrieb ergibt sich aus der funktionalen und organisatorischen Unterschiedlichkeit. So gibt es häufig eine eigene Projektorganisation, die von der Betriebsorganisation abweicht. Gerade bei extern vergebenen Projekten ist zudem noch eine wichtige zivilrechtliche Abgrenzung von Bedeutung. Erst nach der Implementierung und der Abnahme der Prozesse bzw. Systeme geht die Verantwortung auf das auftraggebende Unternehmen über. Eine wesentliche Grundlage für den Projekterfolg sowie die anschließende Wartung und Pflege der Systeme bzw. IT-Prozesse ist die Qualität der erstellten Unterlagen. Qualitativ hochwertige Projektarbeit ist nur möglich, wenn durch die Dokumente die Projektschritte und Projektergebnisse nachvollziehbar sind.

Was bei der Projektdokumentation darüber hinaus zu beachten ist und wie diese strukturiert werden kann, ist Gegenstand von *Kapitel 5*.

2.3 Rahmendokumente

Zusätzlich werden noch Rahmendokumente benötigt. Hierbei kann es sich zum einen um allgemeingültige unternehmensweite Vorgaben (Richtlinien, Leitlinien, Normen u. a.) handeln, die nicht in der Verantwortung der IT-Organisation liegen. Ein typisches Beispiel hierfür ist die Leitlinie zur Informationssicherheit. Diese ist ein Grundsatzdokument der Unternehmensleitung zum Stellenwert von Informationssicherheit, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit.

Zum anderen können auch Dokumente den Rahmendokumenten zugeordnet werden, die Gültigkeit für alle Bereiche der IT-Dokumentation haben und die von der IT-Organisation verantwortet werden. Typischerweise gehören IT-Managementdokumente wie das IT-Risikohandbuch zu den Rahmendokumenten.

Der von den Autoren bewusst gewählte Begriff *Rahmendokumente* (im Gegensatz zum eingrenzenden Begriff *Richtliniendokumente*) soll den weit gefassten und übergreifenden Charakter verdeutlichen.

2.3.1 Rahmendokumente bilden die Klammer

Wie bereits ausgeführt, besteht die IT-Dokumentation neben den Rahmendokumenten aus drei wesentlichen Dokumentationsbereichen:

- Betriebsdokumentation,
- Notfalldokumentation,
- Projektdokumentation.

Bei den Dokumenten, die den genannten drei Bereichen zugeordnet sind, handelt es sich um operative Dokumente. Im Gegensatz dazu sind Rahmendokumente, wie beispielsweise die Leitlinie zur Informationssicherheit oder eine Namenskonvention, allgemeine Regelwerke. Diese regeln übergreifend die allgemeinen Vorgaben und Normierungen.

Die meisten Rahmendokumente sind ein Ergebnis von (IT-)Management-Prozessen. Das IT-Management ist zuständig für die Steuerung der IT. Wie die Steuerung der IT erfolgt, hat ebenfalls Auswirkungen auf die Dokumentation. Viele IT-Organisationen haben eine flache Organisationsstruktur und die IT-Management-Aufgaben liegen bei der Unternehmensleitung. Bei anderen gibt es eine vielschichtige Organisationsstruktur und das IT-Management steuert alle Aufgabenbereiche. Grundsätzlich werden neben der Dokumentation für das Management der Aufbauorganisation daher auch Dokumente für das Management der Ablauforganisation benötigt.

Wichtig ist zum Beispiel die Erstellung eines Organigramms, das den Aufbau der IT-Organisation sowie die Einordnung der IT-Organisation in den Unternehmensstrukturen zeigt. Ein solches Dokument wird beispielsweise im Rahmen des Jahresabschlusses von den Wirtschaftsprüfern gefordert. Zusätzlich sollten die spezifischen Aufgaben in Form von Stellenbeschreibungen dokumentiert werden. Diese müssen Aussagen zu Tätigkeitsmerkmalen, Verantwortungsbereich, Einordnung in die betriebliche Hierarchie, Über- und Unterstellungsverhältnis sowie Stellvertretungsregelungen enthalten.

Aufgabenbereiche des IT-Managements

Gemäß Gabler Wirtschaftslexikon (http://wirtschaftslexikon.gabler.de) können die folgenden vier Aufgabenbereiche des IT-Managements unterschieden werden:

- *IT-Ressourcen-Management:* Das IT-Ressourcen-Management hat die Steuerung von relevanten Ressourcen, z. B. Hardware, Software, Informationen und Personal, zum Inhalt.
- *IT-Servicemanagement:* Dieses dient der Ausrichtung der IT auf ihre Kunden und bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen.
- *IT-GRC-Management:* GRC steht als Zusammenfassung von Governance-, Risk- und Compliance-Management und dient dazu, die IT transparent und damit steuerbar zu machen, Risiken zu planen und sicherzustellen, dass die IT sich konform (compliant) zu internen und externen Regelwerken, insbesondere Gesetzen verhält.
- *IT-Programm- und Portfolio-Management:* Im IT-Progamm- und Portfolio-Management werden konkrete IT-Leistungen mit der IT-Strategie und der Geschäftsstrategie der Kunden und der Gesamtorganisation in Einklang gebracht und in sog. Programme mit ähnlichen Leistungen gruppiert, z. B. Anwendungsentwicklung, Netzwerkbetrieb oder Innovationsberatung. Innerhalb dieser Programme werden später konkrete Leistungen geplant und erbracht. (Wirtschaftslexikon)

2.3.2 Typische Rahmendokumente im Überblick

Für die IT-Dokumentation relevante Rahmendokumente können sowohl auf der Ebene der IT-Dokumentation als auch auf Unternehmensebene verwaltet werden. Hierbei kann es sich, wie bereits beschrieben, um allgemeingültige unternehmensweite Vorgaben (Richtlinien, Leitlinien, Normen u. a.) handeln, sie können aber auch in der Verantwortung der IT-Organisation liegen. Welche Dokumente als Rahmendokumente der IT-Dokumentation zuzuordnen sind, hängt vom Unternehmen und von dessen Verantwortlichkeiten für die Dokumentation ab und muss im Einzelfall betrachtet werden. So ist es möglich, dass bereits Dokumente für das Unternehmen existieren, die auch für die IT-Organisationseinheiten Gültigkeit haben. Ein typisches Beispiel stellt das *Risikohandbuch* dar. Im Rahmen des gesetzlich verankerten Risikomanagements sind Unternehmen verpflichtet, ein Risikomanagement zu betreiben und ein Risikohandbuch mit Maßnahmen zur Risikoerkennung, -steuerung, -quantifizierung, -kommunikation und -kontrolle zu pflegen. Da aber für den Bereich der IT nicht nur unternehmensgefährdende, sondern auch servicegefährdende operative Risiken betrachtet werden müssen, kann es sinnvoll sein, ein gesondertes IT-Risikohandbuch zu führen. Dieses stellt somit eine Detaillierung des unternehmensweiten Risikohandbuchs dar.

Fehlende Standardisierung der Begriffe nicht nur bei den Rahmendokumenten

Leider gibt es keine verbindlichen Definitionen oder Richtlinien für die Verwendung von Dokumentbezeichnungen. Sucht man beispielsweise im Internet nach dem Begriff »IT-Konzept«, findet man mehrere Tausend Einträge. Und fast genauso unterschiedlich ist das, was inhaltlich in einem IT-Konzept dargestellt wird. Während die einen unter einem IT-Konzept ein strategisches Papier der Unternehmensleitung verstehen, verwenden andere den Begriff IT-Konzept als Synonym für das Betriebshandbuch.

Besonders häufig findet der Begriff »Konzept« Verwendung. Gemäß Duden ist ein Konzept ein erster Entwurf bzw. die erste Fassung einer Rede oder eines Schriftstücks. Wikipedia erweitert diese Definition um die Begriffe Plan und Programm für ein Vorhaben. Konzepte haben also grundsätzlich planerischen und strategischen Charakter. Im Rahmen der IT-Dokumentation ist ein Konzept daher zum einen definiert als ein Dokument, das auf der Grundlage der Ausgangssituation und einer Anforderungsanalyse eine technisch zu realisierende Lösung für eine definierte Aufgabe liefert und planerischen Charakter hat.

Zum anderen handelt es sich um Dokumente, die technische und/oder organisatorische Maßnahmen beschreiben und vielfach der Umsetzung einer Richtlinie dienen, etwa zum Thema Informationssicherheit (hier beschreibt das Sicherheitskonzept konkrete Maßnahmen zur Umsetzung der Sicherheitsrichtlinie). Konzepte grenzen sich damit von Richtlinien ab, die allgemeine Anforderungen aus Sicht des Managements für Aufgaben, Abläufe und technische Sachverhalte formulieren. Siehe hierzu auch *Abschnitt 6.2*.

Wichtig ist es in jedem Fall, die Verwendung der Begriffe für das eigene Unternehmen zu definieren. Der folgende Abschnitt möchte für eine derartige Standardisierung Anhaltspunkte liefern. Er stellt wesentliche Rahmendokumente exemplarisch vor und zeigt, wie sich diese Dokumente gegen die übrigen im vorliegenden Buch beschriebenen Dokumentationen abgrenzen. Hierbei werden Dokumente mit den dafür üblicherweise verwendeten Begriffen bezeichnet. Werden für Dokumente in der Literatur bzw. im üblichen Sprachgebrauch verschiedene Namen verwendet, so werden diese (soweit bekannt) zusätzlich angegeben.

In diesem Abschnitt werden einige wichtige Rahmendokumente im Überblick vorgestellt. Dabei geht es nicht um Vollständigkeit. Vielmehr soll die Vorstellung ein Bild vermitteln, welche Dokumente den Rahmendokumenten zugeordnet werden können. Auch steht nicht deren Inhalt oder eine detaillierte Anleitung zur Erstellung im Vordergrund, sondern vielmehr eine Beschreibung der Aufgaben des jeweiligen Rahmendokuments. Dies hat mehrere Gründe: Zum einen könnte allein die Betrachtung des zu den Rahmendokumenten zählenden IT-Risikohandbuchs und der dahinter stehenden Prozesse das Kapitel füllen. Dies würde den Rahmen des Buchs schnell sprengen. Zum anderen gibt es aufgrund der Wichtigkeit der Inhalte dieser Dokumente umfangreiche einschlägige Literatur. Bild 2.7 zeigt

einige wesentliche Rahmendokumente der IT-Dokumentation. Welche Dokumente im Einzelfall zu erstellen sind und ob darüber hinaus noch Dokumente benötigt werden, hängt vom Unternehmen und dessen Aufgaben ab und muss im Einzelfall entschieden werden.

Dokumente können ggf. zusammengefasst werden

Die im Folgenden vorgenommene Unterscheidung in Leitlinien, Richtlinien und Konzepte ist auch den Anforderungen von Normen u. Standards geschuldet, die diese Dokumente zum Teil explizit fordern. Sofern hier keine Verpflichtungen bestehen, können aus Gründen der Praktikabilität Dokumente durchaus zusammengefasst werden. Hinweise zur Strukturierung und Klassifizierung von Dokumenten finden Sie in Abschnitt 6.2.2.

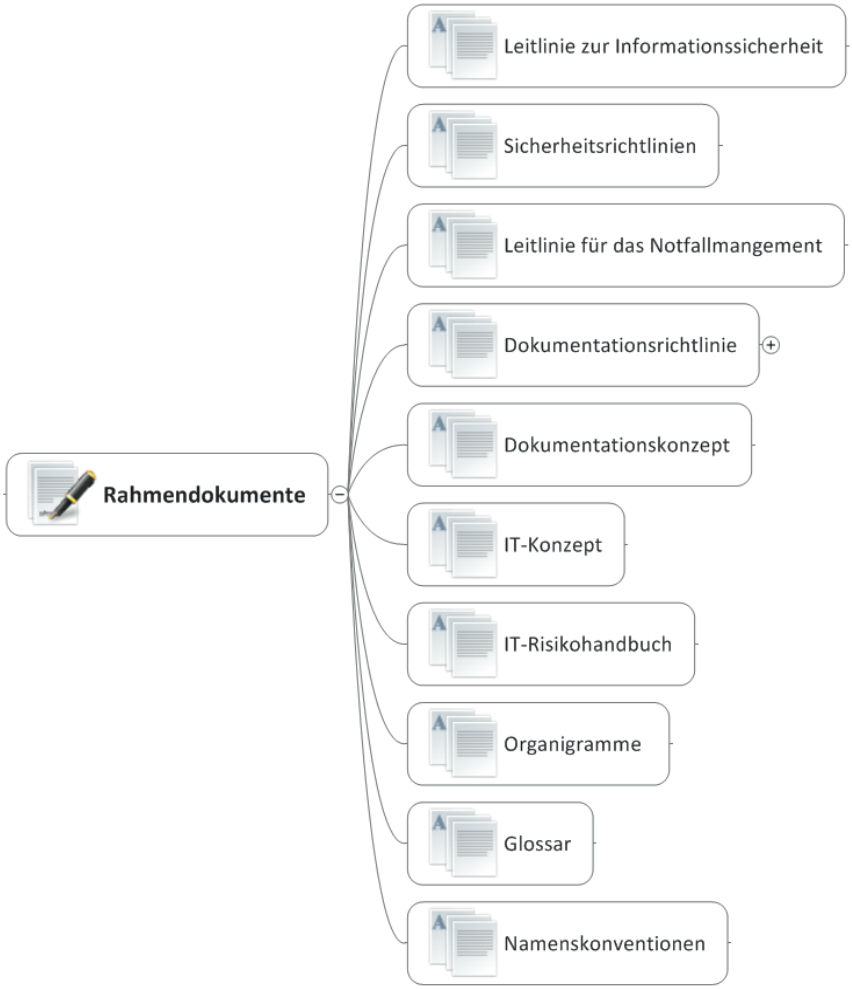


Bild 2.7 Typische Rahmendokumente für die IT-Dokumentation

2.3.2.1 IT-Konzept

Der Begriff IT-Konzept wird sehr unterschiedlich verstanden. Beispielsweise findet man bei Wikipedia eine Gleichsetzung von IT-Konzept mit DV-Konzept: *»Das DV-Konzept (ausführlich Datenverarbeitungskonzept) oder IT-Konzept ist eine Fortführung des Fachkonzeptes bei der Erstellung von Datenbanken oder bei der Programmierung. Es beschreibt die relevanten Daten und deren Verarbeitung. Die im Fachkonzept ermittelten Informationen werden auf die jeweilige Datenbank bzw. Programmiersprache angepasst. Die Aufgabenstellungen aus dem Fachkonzept werden bezüglich der Datenstrukturen und Verarbeitungsschritte strukturiert und dokumentiert«.* (Wikipedia, IT-Konzept)

Im Buch wird mit dem IT-Konzept ein strategisches Dokument bezeichnet, das die Ausrichtung der IT auf die Unternehmensstrategie beschreibt

So wird typischerweise im IT-Konzept festgelegt, ob die IT zentral oder dezentral strukturiert ist und mit welcher Ausprägung.

Es sollte auch für die IT beschreiben, mit welchen Verfahren (z. B. nach welchen Standards) das Unternehmen 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 des Unternehmens. 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 eine mögliche Gliederung für ein Betriebskonzept:

- 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
  - Entscheidungspyramide

Hinsichtlich der Rollenbeschreibungen kann es sinnvoll sein, im IT-Konzept die High-Level-Rollen zu definieren. Dies ersetzt jedoch nicht das in *Abschnitt 3.8.9* beschriebene Rollenkonzept für die Betriebsrollen. Mögliche Rollendefinitionen im IT-Konzept 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 eines Verfahrens verstanden, wenn sie über besondere Kenntnisse im Umgang mit und in den Funktionalitäten des Verfahrens 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.

2.3.2.2 IT-Risikohandbuch

Ein unternehmensweites Risikohandbuch bildet die Grundlage eines unternehmensweiten Risikomanagements. Es stellt organisatorische Maßnahmen und Regelungen dar, die zur Risikoerkennung, -quantifizierung, -kommunikation, -steuerung und -kontrolle zu beachten sind. Zusätzlich liefert dieses Handbuch die Basis für die Prüfung des Risikomanagements, die sowohl extern durch den Abschlussprüfer als auch intern durch die interne Revision oder den Aufsichtsrat vorgenommen werden kann.

Nicht nur das 1998 verabschiedete *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* (siehe *Abschnitt 1.2.3*) fordert, bestehende Risiken aufzuzeigen und der Unternehmensleitung sowie den Anteilseignern oder Investoren transparent zu machen. Während früher aber vor allem Finanzrisiken betrachtet wurden, treten heute zunehmend auch die operativen Risiken in den Vordergrund, wie sie sich beispielsweise aus dem IT-Betrieb ergeben. Zumindest in großen Unternehmen wird deshalb zunehmend vom IT-Bereich ein eigenes IT-Risikohandbuch verlangt.

Aus der historischen Entwicklung heraus ergibt sich ein Problem mit der Abgrenzung zum Sicherheitskonzept. Wie bereits mehrfach betont, bleiben an dieser Stelle nur eine klare Definition der Begrifflichkeiten und die Abgrenzung zu anderen Dokumenten. So kann beispielsweise das IT-Risikohandbuch als Vorgabedokument für das Risikomanagement behandelt werden, während das Sicherheitskonzept einen konkreten Maßnahmenkatalog auf der Grundlage einer Risikoanalyse liefert, die zum Beispiel gemäß BSI-Standard erstellt wurde.

Da die Gewährleistung der Sicherheit ein kontinuierlicher Prozess ist, genügt es nicht, das IT-Risikohandbuch einmal zu erstellen und dann alle Sicherheitsmaßnahmen umzusetzen. Vielmehr muss das Risikomanagement auf neue technische Entwicklungen reagieren und das Risikohandbuch ständig überprüfen und aktualisieren.

Business-Impact-Analyse als Basis der Risikoanalyse

Im Zusammenhang mit der Risikoanalyse taucht häufig der Begriff *Business-Impact-Analyse (BIA)* auf. Was aber verbirgt sich hinter einer »Auswirkungsanalyse«, d. h. einer BIA? Die Business-Impact-Analyse ist eine Methode des Business Continuity Management und dient der Identifizierung und Erfassung der kritischen Geschäftsprozesse eines Unternehmens. Ziel ist es, wechselseitige Abhängigkeiten zwischen den Prozessen und/oder den Unternehmensbereichen aufzuzeigen und die Auswirkungen bei Ausfall von Prozessen bzw. die notwendigen Wiederanlaufzeiten zu ermitteln.

Zusammen mit der Risikoanalyse bildet die BIA die Grundlage für eine effektive Sicherheits- und Notfallvorsorgestrategie und die Basis für das Notfallvorsorgekonzept. Weitere Erläuterungen zur Bedeutung einer Business-Impact-Analyse für das Notfallmanagement finden Sie in *Kapitel 4*. Da es sich bei der Business-Impact-Analyse um eine Unternehmensaufgabe handelt und alle Geschäftsprozesse eines Unternehmens in die Analyse einbezogen werden sollten, sind die dabei entstehenden Dokumente nicht der IT-Dokumentation zuzuordnen.

2.3.2.3 Leitlinie und Richtlinien zur Informationssicherheit

Aufgrund der Bedeutung und der weitreichenden Konsequenzen der zu treffenden Entscheidungen muss der Informationssicherheitsprozess einschließlich dessen Teilbereich IT-Sicherheit (wie auch der Notfallmanagementprozess) von der obersten Leitungsebene initiiert, gesteuert und kontrolliert werden. Zu verankern ist die Verantwortung der Unternehmensleitung in entsprechenden Leitlinien.

Die **Leitlinie** zur Informationssicherheit ist demzufolge ein strategisches Unternehmensdokument, das die zentralen Ziele für die Informationssicherheit in einem Unternehmen festschreibt. Sie definiert die Sicherheitsziele und die Grundsätze für den Umgang mit Informationen sowie die Verantwortungsbereiche für die Informationssicherheit. Sinnvollerweise sollte die Leitlinie zur Informationssicherheit Bestandteil einer übergeordneten Sicherheitsleitlinie sein.

Für eine Sicherheitszertifizierung nach ISO 27001 oder BSI-Grundschutz ist die Leitlinie zur Informationssicherheit ein unverzichtbares Dokument und muss gemäß BSI Standard 100-1 Aussagen zu den nachfolgenden Punkten enthalten:

- Ziele und Strategien des Unternehmens in Bezug auf die Informationssicherheit unter Berücksichtigung geschäftlicher, gesetzlicher und vertraglicher Sicherheitsverpflichtungen,
- Beziehung der Sicherheitsziele zu den Geschäftszielen,
- angestrebtes Sicherheitsniveau,

- Leitaussagen, wie das angestrebte Sicherheitsniveau erreicht werden soll,
- Leitaussagen, ob und wodurch das Sicherheitsniveau nachgewiesen werden soll, und
- Organisationsstruktur für die Umsetzung der Leitlinie zur Informationssicherheit und Benennung der Verantwortlichen (u. a. Ernennung eines Sicherheitsbeauftragten).

Dabei beschreibt die Leitlinie keine Details, sondern macht grundsätzliche Aussagen, ohne diese zu spezifizieren. Sie sollte kurz und prägnant sein und wird in der Regel nur selten geändert.

Ergänzt wird die Sicherheitsleitlinie durch eine oder mehrere **Sicherheitsrichtlinien**. So fordert die ISO 27001 beispielsweise u. a. die Erstellung folgender Richtliniendokumente:

- Richtlinie für Zugriffsrechte und den Umgang mit Passwörtern,
- E-Mail-Richtlinie,
- Internetrichtlinie,
- Remote-Access-Richtlinie,
- Antivirus-Richtlinie,
- Richtlinie für Lieferanten und Provider.

Bei den genannten Sicherheitsrichtlinien handelt es sich jedoch um operative Dokumente, da sie konkrete Anweisungen und Festlegungen enthalten. Sie können daher auch der Betriebsdokumentation zugeordnet werden.

Weiterhin wird ein **Sicherheitskonzept** benötigt. Dieses regelt die Struktur und die konkrete Umsetzung der Informationssicherheit (Erläuterungen zum Sicherheitskonzept finden Sie in *Abschnitt 3.8.13*). Während also die Leitlinie Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben des Unternehmens vorgibt, beschreibt das Sicherheitskonzept detaillierte Sicherheitsmaßnahmen und Handlungsanweisungen zur Umsetzung der Leitlinie und der Richtlinien.

Wie alle Rahmendokumente müssen die Leitlinie zur Informationssicherheit und die Richtlinien sowohl in regelmäßigen Abständen wie auch anlassbezogen bei Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder Strategien auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Zu empfehlen ist ein Review-Zyklus von zwei Jahren.

2.3.2.4 Dokumentationsrichtlinie

Mit wachsender Unternehmensgröße werden die Erstellung und die Durchsetzung einer Dokumentationsrichtlinie zunehmend wichtiger. Diese wird sinnvollerweise übergeordnet auf Unternehmensebene definiert. Wo eine solche übergeordnete Richtlinie fehlt, sollte sie für die IT-Organisation erstellt werden. Sinnvollerweise wird zusätzlich zur Richtlinie ein Dokumentationskonzept erstellt, das die operativen Vorgaben für die Dokumentation definiert (siehe hierzu *Abschnitt 6.2.22*).

Die Aufgabe einer Dokumentationsrichtlinie ist es, übergeordnete Regelungen für die Dokumentation festzulegen. Sie sollte mindestens folgende Punkte regeln:

- Abgrenzung der Dokumentation,
- Verantwortlichkeiten,
- übergeordnete Regelungen zur Dokumentenverwaltung.

Weitergehende Informationen zu den möglichen Inhalten einer Dokumentationsrichtlinie sowie zum Thema Standardisierung finden Sie in *Abschnitt 6.2.1.*

2.3.2.5 Glossar

Ein Glossar ist definiert als eine Zusammenstellung ausgewählter (Fach-)Begriffe, die mit knappen Sätzen erklärt werden. Handelt es sich dabei um Fremdwörter oder Wörter in einer anderen Sprache, ist zusätzlich eine Übersetzung sinnvoll.

Üblicherweise befindet sich in Dokumenten im Anhang ein Glossar, das die im Dokument verwendeten Fachbegriffe und Abkürzungen erläutert. Es soll den richtigen Gebrauch der Fachausdrücke und deren eindeutiges Verständnis sicherstellen. Wichtig ist dabei, dass das Glossar definiert, wie die Begriffe im betreffenden Dokument verwendet werden. So gibt es viele Fachbegriffe, die nicht eindeutig definiert sind. Für diese Fälle ist es zwingend erforderlich, im Glossar deren jeweilige Verwendung im Dokument zu erläutern.

Um eine einheitliche Verwendung von Begriffen sicherzustellen, ist die Pflege eines zentralen Glossars sinnvoll. Dieses sollte für den IT-Bereich auch die Verwendung von Dokumentenbezeichnungen definieren und diese deutlich voneinander abgrenzen. Weiter muss die verbindliche Verwendung der Begriffe kommuniziert und sichergestellt werden, dass jeder, der Dokumente erstellt, die Bezeichnungen wie definiert verwendet.

Wird ein zentrales Glossar gepflegt, ist in den Dokumenten nur dann ein Glossar notwendig, wenn das Dokument (auch) extern Verwendung findet.

Wie wichtig ein Glossar ist, kann man an diesem Buch ablesen, in dem ein nicht kleiner Teil dafür aufgewendet wird, die verwendeten Begriffe zu erklären und Abgrenzungen festzulegen.

Glossar im Anhang

Im Anhang finden Sie ein Glossar mit Erläuterungen der wesentlichen im Buch verwendeten Fachbegriffe. Die nachstehenden Begriffe dienen dem Verständnis der Beiträge im Buch und stellen eine Auswahl der wichtigsten Begriffe dar.
Ein erweitertes Glossar finden Sie auf unserem Blog unter http://www.itdoku-kompakt.de.

2.3.2.6 Namenskonventionen

Auf den ersten Blick mögen Namenskonventionen zweitrangig erscheinen, jedoch wird ihre Bedeutung häufig unterschätzt. Namenskonventionen gehören vielmehr zu den wichtigsten Rahmendokumenten. Die Erarbeitung und die Umsetzung von Namenskonventionen sind der erste Schritt zur Erreichung einer konsistenten IT-Dokumentation.

Beispielsweise ist ein im Vorfeld sorgfältig geplantes, einheitliches Schema der Namenskonventionen für alle Objekte der Active-Directory-Gesamtstruktur insbesondere in großen Unternehmen unerlässlich, um Wildwuchs mit entsprechend eingeschränkter Nachvollziehbarkeit bei den Objektbezeichnungen zu vermeiden. Wichtig ist, dass alle mit der Vergabe von Namen betrauten Mitarbeiter von den Regelungen – dies gilt vor allem auch für externe Berater – Kenntnis haben und sie auch anwenden.

Die nachstehende Aufstellung zeigt beispielhaft die wichtigsten Systeme und Komponenten, für die typischerweise in einer Active-Directory-Umgebung die Namen standardisiert werden sollten. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit und muss im Einzelfall angepasst werden.

- Server,
- Cluster-Systeme (virtuelle Server und Cluster-Knoten),
- Linux-/UNIX-Server,
- Clients,
- Domänen (Root-Domäne und Sub-Domänen),
- Standorte im Active Directory (Standorte, Standort-Links und Standorteigenschaften),
- Organisationseinheiten (OUs),
- Gruppenrichtlinien (GPOs),
- Gruppen,
- Benutzer (Anmeldename, angezeigter Name, E-Mail-Adresse, Beschreibung),
- administrative Benutzer (Anmeldename, angezeigter Name, E-Mail-Adresse, Beschreibung),
- Funktionsbenutzer, z. B. Hotline-Benutzer (Anmeldename, angezeigter Name, E-Mail-Adresse, Beschreibung),
- Dienstkonten,
- Dateinamen, Verzeichnisnamen, Freigabebezeichnungen, persönliche Ordner, servergespeicherte Benutzerprofile,
- Drucker (Druckername, Druckerstandort),
- Messaging-Dienst, z. B. Exchange (Exchange-Server-Name, Routing Group, Connectoren, öffentliche Ordner, Verteilerlisten, persönliche Postfächer, Postfach-Alias, Funktionspostfächer).

Sind für die Produktionsumgebung und die Testumgebung unterschiedliche Namenskonventionen erforderlich, sollte dies entsprechend berücksichtigt werden.

Daneben gibt es für den IT-Betrieb aber noch weitere Komponenten, für die eine Standardisierung von Namen sinnvoll ist. Hierzu zählen beispielsweise Konventionen zur Benennung von Prozessen und Unterprozessen sowie Regelungen zur Benennung von Rollen (beispielsweise ob englische oder deutsche Bezeichnung). Und schließlich sollten für Dokumente verbindliche Namensregeln (sowohl für Dokumententitel als auch für Dateinamen) festgelegt werden (*siehe Abschnitt 6.2*).

2.4 Abgrenzung zur technischen Dokumentation

Die in den vorstehenden Kapiteln dargestellte Struktur mag fälschlicherweise den Eindruck erwecken, dass damit alle Dokumentationsbereiche für IT- und Anwendungssysteme erfasst sind. Es gibt aber noch eine Reihe weiterer Dokumentationsfelder mit Bezug zur IT, die im Buch nicht berücksichtigt werden. Hierzu gehört der Bereich der Produktdokumentation. Dieser stellt ein eigenständiges Aufgabengebiet mit speziellen Anforderungen und Vorgaben dar und wird der technischen Dokumentation zugeordnet.

Die nachstehenden Ausführungen sollen einen Überblick über die Aufgabenbereiche der technischen Dokumentation vermitteln. Für weitere Informationen sei auf die zahlreich vorhandene Spezialliteratur verwiesen.

Definition »Technische Dokumentation«

Wohl jeder hat schon einmal über die scheinbar banalen Sicherheitshinweise geschmunzelt, die in der mehrsprachigen Bedienungsanleitung auch einfachster Produkte zu finden sind. Diese sind jedoch keineswegs banal, sondern basieren auf einer ganzen Reihe gesetzlicher Anforderungen. Die Erstellung derartiger Anleitungen gehört in den Bereich der technischen Dokumentation.

Die Erstellung von Gebrauchsanweisungen für technische Produkte ist aber nur ein Teilbereich. Vielmehr ist der Begriff *Technische Dokumentation* der allgemeine Oberbegriff für die Dokumentation zu einem Produkt. Diese umfasst eine Reihe an Unterlagen, die beispielsweise eine Herstellerfirma für ihr Produkt bereitzustellen hat:

- Bedienungsanleitungen,
- Betriebsanleitungen,
- Serviceanleitungen,
- Installationshandbücher,
- Softwarehandbücher,
- …

Diese Liste ist jedoch keineswegs vollständig, wie Bild 2.8 zeigt und einen Eindruck von der Vielschichtigkeit der Produktdokumentation vermittelt.

Eine Definition des Begriffs Technische Dokumentation, die anschaulich deren Aufgaben beschreibt, gibt Josef Grupp in seinem *Handbuch Technische Dokumentation*:

> *»Technische Dokumentation ist die geordnete Zusammenstellung ausgewählter Dokumente und Sprachmaterialien des Herstellers zu einem von ihm erstellten technischen Produkt, mit der er dem Verwender des Produkts den sicheren und nützlichen Umgang vermittelt und mit der er dem Gesetzgeber ein beweiskräftiges Zeugnis für die Erfüllung der gesetzlichen Anforderungen liefert bzw. ihm einen anschaulichen Beweis für die Erfüllung dieser Anforderungen gibt.«* (Grupp, 2008)

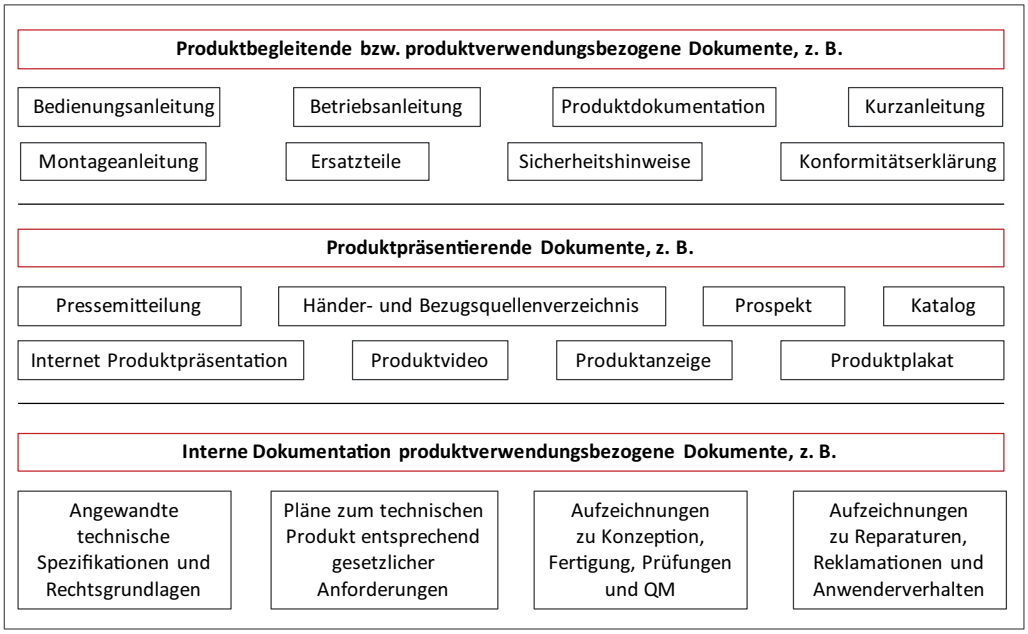


Bild 2.8 Teile der technischen Dokumentation nach (Grupp, 2008)

Die *tekom*, der deutsche *Fachverband für Technische Kommunikation und Informationsentwicklung*, benennt darüber hinaus in ihrer Definition die verschiedenen Zwecke, für die technische Dokumente benötigt werden. Hierzu gehören: Produktdefinition und Produktspezifikation, Konstruktion, Herstellung, Qualitätssicherung, Produkthaftung, Produktdarstellung, Beschreibung von Funktionen und Schnittstellen, bestimmungsgemäße, sichere und korrekte Anwendung, Instandhaltung und Reparatur eines technischen Produkts sowie gefahrlose Entsorgung.

Notwendigkeiten zur Erstellung einer technischen Dokumentation ergeben sich demzufolge aus einer ganzen Reihe von Anforderungen. Um beispielsweise die Sicherheit von Produkten sicherzustellen, fordern Gesetze und Vorschriften privatrechtlicher Organisationen entsprechende Dokumente von Seiten der Hersteller. Hierzu gehören in der EU Richtlinien wie die *Maschinenrichtlinie* oder die Produktsicherheitsrichtlinie, die in Deutschland in Form des *Produktsicherheitsgesetzes (ProdSG)* in nationales Recht umgesetzt wurden. Das ProdSG ersetzt seit 1. Dezember 2011 das Geräte- und Produktsicherheitsgesetz (GPSG). Es regelt die Sicherheitsanforderungen an technische Arbeitsmittel und Verbraucherprodukte und verpflichtet Hersteller und Händler, sichere Produkte auf den europäischen Markt zu bringen. Als ein wesentliches Kriterium für die Beurteilung der Sicherheit von Produkten nennt § 3, Absatz 2, Ziffer 3 GPSG ausdrücklich die Gebrauchs- und Bedienungsanleitung und die sonstigen produktbezogenen Angaben oder Informationen, insbesondere Warnhinweise. Und § 2, Absatz 4 ProdSG betont, dass eine Gebrauchsanleitung in deutscher Sprache dem Produkt beizuliegen hat.

Es gibt aber nicht nur zahlreiche Gesetze und Richtlinien, die die Verpflichtung zur Erstellung der Dokumentation regeln, sondern auch zahllose branchenbezogene Normen und Richtlinien, die eine Standardisierung sicherstellen und die Gestaltung technischer Doku-

mente regeln. In diesem Punkt unterscheidet sich die IT-Dokumentation sehr deutlich von der technischen Dokumentation.

Software als Produkt

Auch die Softwaredokumentation wird zumindest rechtlich der technischen Dokumentation zugeordnet, denn demnach handelt es sich bei einer Software um ein Produkt, für das alle Aspekte von Verbraucherschutz, Haftung und Gewährleistung u. a. zum Tragen kommen und für das eine entsprechende Dokumentation zu erstellen ist. Das findet seinen Niederschlag in zahlreichen Normen und Standards zur Softwaredokumentation. Hierzu zählen u. a. die folgenden:

- *»ISO/IEC 26514:2008 System and Software Engineering – Requirements for designers and developers of user documentation Die Norm ist eine Zusammenfassung und Aktualisierung der Normen IEEE 1063:2001 und ISO/IEC 18019:2004. Sie enthält sowohl die Richtlinien für den Erstellungsprozess als auch die Kriterien für das Dokumentationsprodukt.*
- *IEEE 1063:2001 Software user documentation Die internationale Norm beschreibt, wie eine qualitativ gute Softwaredokumentation aufgebaut und gestaltet sein sollte. Die Norm greift sowohl die Dokumentation in Papierform als auch elektronische Medien auf. Die Norm gliedert sich in Forderungen an Struktur, Inhalt und Form von Softwaredokumentation«* (Grünwied, 2009)

Die vollständige Dokumentation zu einem Softwareprodukt besteht demzufolge aus unterschiedlichen Teilen, die auf verschiedene Zielgruppen ausgerichtet sind:

- Programmiererdokumentation,
- Methodendokumentation,
- Installationsdokumentation,
- Benutzerdokumentation,
- Datendokumentation,
- Testdokumentation,
- Entwicklungsdokumentation.

Weiterführende Dokumentation

Die vorgestellten Anforderungen an eine technische Dokumentation sind für Sie relevant, wenn Sie beispielsweise Software entwickeln und vertreiben. Nähere Informationen zur Technischen Dokumentation und zu den Anforderungen an die Produktdokumentation finden Sie auf der Website der tekom unter dem folgenden Link: http://www.tekom.de.

Außerdem finden Sie in *Abschnitt 5.4* grundsätzliche Informationen zur Anwendungsdokumentation.

2.5 Zusammenfassung

Aus den Ausführungen der vorstehenden Kapitel lassen sich für den Bereich der IT-Dokumentation vier wesentliche Dokumentationsbereiche ableiten:

- Rahmendokumente,
- Betriebsdokumentation,
- Notfalldokumentation,
- Projektdokumentation.

Die in Bild 2.4 gezeigte Struktur bildet die Basis für das vorliegende Buch. Wie in diesem Kapitel gezeigt wurde, gibt es eine Reihe von Dokumenten, die übergeordneten Charakter haben und Regelungen und Richtlinien definieren. Sie werden im vorliegenden Buch als *Rahmendokumente* bezeichnet. In den folgenden Kapiteln werden die weiteren Dokumentationsbereiche ausführlich vorgestellt. Die Beschreibung beinhaltet sowohl Erläuterungen zu deren Strukturierung als auch Anleitungen zur Erstellung der erforderlichen Dokumente.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z