

Manuela Reiss
Georg Reiss

Praxisbuch IT-Dokumentation

Betriebshandbuch, Systemdokumentation
und Notfallhandbuch im Griff



3

Rahmendokumente

Vielfach werden Dokumente ausschließlich vor dem Hintergrund einer technischen Lösung für eine bestehende Anforderung erstellt. Dabei wird häufig vergessen, dass die wenigsten Lösungen für sich stehen, sondern in einem Systemverbund funktionieren müssen. Aus diesem Grund werden zusätzlich *Rahmendokumente* benötigt, die die organisatorischen und betrieblichen Belange regeln und eine funktionierende Gesamtkonzeption sicherstellen. Ein typisches Beispiel hierfür ist das IT-Sicherheitskonzept. Seine Hauptaufgabe ist es, den Schutzbedarf der IT-Anwendungen und IT-Systeme für alle Bereiche festzustellen und dafür angemessene Sicherheitsmaßnahmen vorzusehen.

Das folgende Kapitel stellt die wichtigsten der für die IT-Dokumentation relevanten Rahmendokumente vor und zeigt, wie sich diese Dokumente gegen die übrigen im vorliegenden Buch beschriebenen Dokumente abgrenzen.

3.1 Rahmendokumente bilden die Klammer

Bevor die Rahmendokumente im Einzelnen vorgestellt werden, gilt es zunächst zu klären, was überhaupt ein Rahmendokument ist.

3.1.1 Einordnung der Rahmendokumente

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

- ▶ Betriebshandbuch
- ▶ Notfallhandbuch
- ▶ Projektdokumentation

Bei den Dokumenten, die diesen drei Bereichen zugeordnet sind, handelt es sich um tätigkeitsbezogene Dokumente.

Klammer für
alle anderen
Dokumente

Im Gegensatz dazu handelt es sich bei den Rahmendokumenten, wie beispielsweise dem IT-Konzept oder einer IT-Namenskonvention um Regelwerke. Diese regeln übergreifend zum einen die allgemeinen Vorgaben und Normierungen und legen zum anderen Zuordnungen (beispielsweise Zuordnungen von Mitarbeitern zu Rollen) fest. Damit stellen die Rahmendokumente eine Klammer für die anderen Dokumente einer Dokumentation dar.

Die Aufgaben der einzelnen Rahmendokumente können dabei sehr unterschiedlich sein. Während einige überwiegend strategischen Charakter haben, wie beispielsweise das IT-Konzept, haben andere Dokumente direkten Einfluss auf den operativen Betrieb. Zu Letzteren zählen beispielsweise das Berechtigungskonzept und die Betriebsmatrix.

Welche Dokumente als Rahmendokumente der IT-Dokumentation zuzuordnen sind, hängt vom Unternehmen und dessen Dokumentenverwaltung ab und muss im Einzelfall betrachtet werden.

Unternehmens-
weit gültige
Dokumente

So ist es möglich, dass bereits Dokumente für das Unternehmen existieren, die auch für die IT-Organisationseinheiten Gültigkeit haben. Ein typisches Beispiel stellt das Projektmanagement-Handbuch dar. Insbesondere große Unternehmen verfügen häufig über ein solches Dokument, das die Verfahren festlegt, nach denen Projekte im Unternehmen durchzuführen sind. Möglich ist aber auch, dass das unternehmensweite Projektmanagement-Handbuch lediglich allgemeine Vorgaben macht (beispielsweise die Projektorganisation vorgibt), für IT-Projekte aber zusätzlich ein gesondertes IT-Projektmanagement-Handbuch existiert. In Letzterem kann beispielsweise festgelegt werden, dass IT-Projekte grundsätzlich nach dem PRINCE2-Projektmodell durchzuführen sind.

Ein weiteres Beispiel eines unternehmensweiten Dokuments ist das Risikohandbuch für das Unternehmen. Im Rahmen des gesetzlich verankerten Risikomanagements pflegen viele Unternehmen ein unternehmensweites Risikohandbuch. Dieses muss unternehmensgefährdende Risiken enthalten. Da aber für den Bereich der IT nicht nur unternehmensgefährdende, sondern auch servicegefährdende Risiken betrachtet werden müssen, kann es sinnvoll sein, ein gesondertes IT-Risikohandbuch zu führen. Dieses stellt somit eine Detaillierung des unternehmensweiten Risikohandbuches dar.

3.1.2 Begriffsschaos nicht nur bei den Rahmendokumenten

Besonders beliebt ist für Dokumente, die dem Bereich der Rahmendokumente zuzuordnen sind, der Begriff *Konzept* (Berechtigungskonzept, Sicherheitskonzept, Administrationskonzept, Rollenkonzept, IT-Konzept). Dabei können die meisten dieser Dokumente kaum der später im Buch noch zu erörternden Kategorie „Konzepte“ zugeordnet werden.

Was ist ein Konzept?

Dass beispielsweise ein IT-Berechtigungskonzept mit verbindlichen Regelungen zu Zugriffsberechtigungen nichts mit einem Konzept gemein hat, wird deutlich, wenn man sich die Definition von Konzept betrachtet. Gemäß dem 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.

Verschärft wird die Situation noch dadurch, dass es keine verbindliche Definition oder Richtlinien für die Verwendung von Dokumentbezeichnungen gibt. Sucht man 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.

Die vorstehenden Beispiele verdeutlichen, dass man von einer Normung von Dokumentbezeichnungen gerade im Bereich der IT weit entfernt ist. Es ist daher dringend zu empfehlen, beim Aufbau der eigenen IT-Dokumentation die Verwendung der Dokumentbezeichnungen für das eigene Unternehmen zu definieren und diese deutlich von einander abzugrenzen. Weiter muss die verbindliche Verwendung der Begriffe kommuniziert und sichergestellt werden, dass jeder, der Dokumente erstellt, die Bezeichnungen wie definiert verwendet.

Eigene Standards festlegen

Das folgende Kapitel möchte für eine derartige Standardisierung einige Anhaltspunkte liefern. Es stellt die wichtigsten Rahmendokumente exemplarisch vor und zeigt, wie sich diese Dokumente gegen die übrigen im vorliegenden Buch beschriebenen Dokumentationen abgrenzen.

hinweis

Für die Verwendung von Dokumentbezeichnungen im Buch gilt Folgendes:

Dokumente werden mit den dafür üblicherweise verwendeten Begriffen bezeichnet. Werden für Dokumente in der Literatur üblicherweise auch andere Namen verwendet, so werden diese (soweit bekannt) zusätzliche angegeben. Beispielsweise wird der Begriff IT-Rahmenkonzept manchmal anstelle von IT-Konzept verwendet.

Diese Vorgehensweise gilt auch für Dokumente mit dem Begriff „Konzept“ im Namen wie beispielsweise Sicherheitskonzept und Berechtigungskonzept, auch wenn sie definitionsgemäß keine Konzepte sind.

3.2 Die Rahmendokumente im Überblick

In diesem Kapitel werden einige wichtige Rahmendokumente der IT-Dokumentation im Überblick vorgestellt. Dabei steht nicht eine detaillierte Anleitung zu deren Erstellung im Vordergrund, sondern vielmehr eine Beschreibung der Aufgaben des jeweiligen Rahmendokuments. Dies hat mehrere Gründe: Zum einen könnte allein beispielsweise die Betrachtung des zu den Rahmendokumenten zählenden IT-Risikohandbuches und der dahinterstehenden Prozesse das Kapitel füllen. Dies würde den Rahmen des Buches schnell sprengen. Zum anderen gibt es aufgrund der Wichtigkeit dieser Dokumente zu den meisten der Rahmendokumente eine umfangreiche Literatur.

Die nachstehende Grafik zeigt die wichtigsten 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.

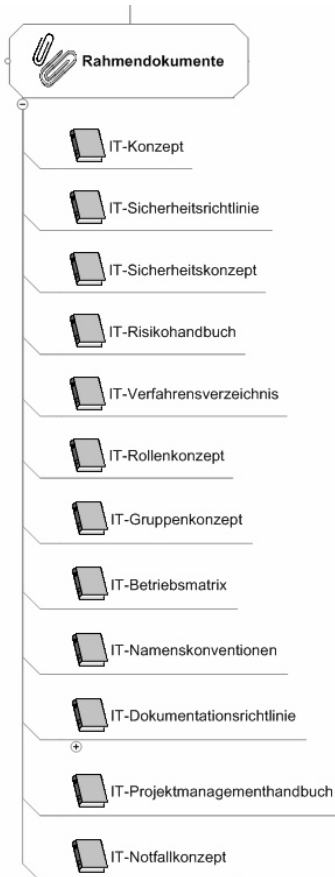


Abbildung 3.1: Wichtige Rahmendokumente der IT-Dokumentation

3.2.1 IT-Konzept

» Für *IT-Konzept* häufig synonym verwendete Begriffe: IT-Betriebskonzept, IT-Rahmenkonzept, Betriebskonzept. Auch das „Betriebshandbuch“ « wird manchmal als IT-Konzept bezeichnet.

Das IT-Konzept ist ein strategisches Dokument, das der grundsätzlichen Einordnung der IT in das Unternehmen dient und die übergeordnete strategische Ausrichtung des Unternehmens im Hinblick auf die IT festlegt. 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 welcher Technik und welchen Verfahren das Unternehmen welche Zwecke verfolgt. Damit soll 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.

3.2.2 IT-Sicherheitsrichtlinie

» Für *IT-Sicherheitsrichtlinie* synonym verwendete Begriffe: Sicherheits-Policy, Security Policy, Sicherheitsleitlinie «

Die IT-Sicherheitsrichtlinie schreibt die zentralen Richtlinien für die IT-Sicherheit in einem Unternehmen fest. Sie definiert die Sicherheitsziele und die Grundsätze für den Umgang mit Informationen sowie die Verantwortungsbereiche für die IT-Sicherheit. Vor allem für große Unternehmen ist der Einsatz einer Sicherheitsrichtlinie wichtig, um übergreifende IT-Sicherheitsregeln unternehmensweit durchzusetzen. So kann beispielsweise in der Sicherheitsrichtlinie festgelegt werden, dass unternehmensweit ausschließlich vom Unternehmen bereitgestellte Rechnersysteme und Speichersysteme eingesetzt werden dürfen und technisch sicherzustellen ist, dass keine Fremdrechner Zugang zum lokalen Netzwerk erhalten.

Kleinere Unternehmen können zwar gegebenenfalls auf eine IT-Sicherheitsrichtlinie verzichten, sollten aber in jedem Fall ein IT-Sicherheitskonzept erstellen, das dann zusätzlich die übergeordneten Richtlinien beinhalten kann.

Gemäß den Empfehlungen des BSI (hier wird sie als IT-Sicherheitsleitlinie bezeichnet) sollte die IT-Sicherheitsrichtlinie Aussagen zu den nachfolgenden Punkten enthalten:

Inhalt der IT-Sicherheitsrichtlinie

- ▮ Bedeutung der IT-Sicherheit für die Geschäftsprozesse
- ▮ Ziele und Strategien des Unternehmens in Bezug auf die IT-Sicherheit

- Organisationsstruktur für die Umsetzung der IT-Sicherheitsrichtlinie und Benennung der Verantwortlichen (zum Beispiel die Ernennung eines IT-Sicherheitsbeauftragten)
- Maßnahmen zur regelmäßigen Überprüfung der Einhaltung der Sicherheitsstandards

Entsprechend dem IT-Konzept beschreibt die IT-Sicherheitsrichtlinie keine Details, sondern macht grundsätzliche Vorgaben, ohne diese zu spezifizieren. Sie sollte kurz und prägnant sein. Sie wird in der Regel sehr selten geändert.

3.2.3 IT-Sicherheitskonzept

» Für *IT-Sicherheitskonzept* synonym verwendete Begriffe: Sicherheitskonzept, Sicherheitshandbuch. «

Das IT-Sicherheitskonzept regelt die Struktur und die konkrete Umsetzung der IT-Sicherheit. Fälschlicherweise wird das IT-Sicherheitskonzept manchmal auch als IT-Sicherheitsrichtlinie bezeichnet, obwohl es sich klar von dieser abgrenzen lässt. Während die Richtlinie Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben des Unternehmens vorgibt, beschreibt das IT-Sicherheitskonzept detaillierte Sicherheitsmaßnahmen und Handlungsanweisungen zum Umgang mit IT-Sicherheit. Eine durchaus sinnvolle Alternative ist hingegen die Verwendung des Begriffs IT-Sicherheitshandbuch.

Zu kaum einem anderen sicherheitsrelevanten Dokument findet man so viele Informationen und Beispiele, wie zum IT-Sicherheitskonzept. Dies liegt vor allem an seiner Bedeutung. Das IT-Sicherheitskonzept ist für ein Unternehmen erforderlich, damit konkrete Sicherheitsmaßnahmen geplant, umgesetzt und später aktualisiert werden können. Es ist „das“ zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen.

Wichtiger
Baustein im
IT-Grundschutz

Zum anderen ist das IT-Sicherheitskonzept ein zentraler Bestandteil im IT-Grundschutz gemäß BSI (siehe hierzu Abschnitt 1.2.3) und dort ausführlich beschrieben. Gemäß IT-Grundschutzhandbuch werden im IT-Sicherheitskonzept die Risiken für die Geschäftsprozesse, IT-Anwendungen und IT-Systeme bewertet. Ebenso wird konzipiert, welche Sicherheitsmaßnahmen einen angemessenen Schutz bieten.

3.2.3.1 Inhalt des IT-Sicherheitskonzepts

Die Basis für jede Risikobewertung ist die genaue Kenntnis der zu schützenden Systeme, Anwendungen und IT-Prozesse. Aufbauend auf einer Dokumentation aller Systeme sollte das IT-Sicherheitskonzept eine Auflistung der vorhandenen Schwachstellen, der möglichen Bedrohungen und der bereits umgesetzten Maßnahmen liefern. Das BSI empfiehlt, die genannten Punkte für sämtliche IT-Systeme und Prozesse zu beschreiben und die Maßnahmen umzusetzen. Zusätzlich wird für Komponenten mit hohem oder sehr hohem Schutzbedarf empfohlen, eine weitergehende Sicherheitsanalyse durchzuführen.

IT-Grundschutz nach BSI

Mit der Version 2005 hat das BSI das ehemalige „IT-Grundschutzhandbuch“ zugunsten einer Zweiteilung aufgegeben. In der Neufassung gibt es zum einen ein Handbuch mit den Standards 100-1 bis 100-3 (der Standard 100-4 liegt derzeit als Entwurf vor), das die grundsätzlichen Anforderungen und Vorgehensweisen nach IT-Grundschutz sowie zur Risikoanalyse beschreibt. Zum anderen wurden aus den Bausteinen und Maßnahmen die IT-Grundschutz-Kataloge in Form einer Loseblattsammlung erstellt. Standards und Kataloge bilden dabei eine inhaltliche Einheit, wobei die Standards die Klammer um die Grundschutz-Kataloge bilden.

Die Erfassung aller vorhandenen IT-Systeme ist demzufolge eine Grundvoraussetzung für die Erstellung eines wirksamen IT-Sicherheitskonzepts. Es ist jedoch nicht sinnvoll, diese in das Sicherheitskonzept aufzunehmen. Wird der im vorliegenden Buch entwickelte Ansatz einer Systemdokumentation als Bestandteil des Betriebshandbuches umgesetzt, stellt dies gleichzeitig die Basis für die Risikoanalyse und aller anderen Grundschutzmaßnahmen dar. Eine ausführliche Beschreibung der Systemdokumentation finden Sie in Abschnitt 4.2.

Systemdokumentation
als Basis

Für die Erstellung eines IT-Sicherheitskonzepts bietet sich nachfolgende Vorgehensweise an, die gleichzeitig eine sinnvolle Strukturierung des IT-Sicherheitskonzepts darstellt. Diese folgt weitgehend den Vorgaben des BSI-Standards. Bei dieser Vorgehensweise wird vorausgesetzt, dass eine Systemdokumentation und eine Dokumentation der IT-Prozesse vorliegen:

Der Weg zum
IT-Sicherheitskonzept

1. **Schutzbedarfsfeststellung:** Die Schutzbedarfsfeststellung umfasst drei Schritte. Im Vordergrund steht dabei die Fragestellung, wie groß der maximale Schaden ist, wenn die Verfügbarkeit, die Integrität oder die Vertraulichkeit der zu untersuchenden IT-Systeme und Informationen beeinträchtigt werden:
 - Analyse, welche Gefährdungen bzw. Risiken für das Unternehmen bei unzureichender IT-Sicherheit bestehen
 - Identifizierung möglicher Schäden durch einen Verlust an Vertraulichkeit, Integrität oder Verfügbarkeit
 - Analyse und Bewertung der potenziellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch IT-Sicherheitsvorfälle und andere IT-Sicherheitsrisiken

2. *Bewertung der erfassten IT-Systeme und IT-Prozesse:* Im nächsten Schritt werden die Systeme bewertet und kategorisiert. Dazu werden die in der Schutzbedarfsfeststellung identifizierten Risiken auf die erfassten IT-Systeme angewendet und für die darauf verarbeiteten Informationen die Maximalschäden bestimmt. Dies schließt die Identifikation und Beurteilung sicherheitsrelevanter Informationen, Geschäftsprozesse und organisatorischer Abläufe ein. Ziel ist, Systeme und Prozesse mit gängigen Risiken von denen mit hohen oder sehr hohen Risiken zu unterscheiden.
3. *Sicherheits-Ist-Analyse/Risikoanalyse:* Im nächsten Schritt sind die vorhandenen Sicherheitsmaßnahmen zu erfassen und mögliche Defizite aufzuzeigen (Soll-Ist-Vergleich). Auch hierbei ist eine Unterteilung sinnvoll. Diese kann wie folgt aussehen:
 - Vorhandene Sicherheitsmaßnahmen und Risiken übergeordneter Komponenten mit hohem Schutzbedarf (Organisation, Personal, Notfallvorsorge, Datensicherung, Datenschutz)
 - Vorhandene Sicherheitsmaßnahmen und Risiken von Infrastruktur-Komponenten (Gebäude, Verkabelung, Büroräume, Serverräume/Rechenzentrum, Datenträgerarchiv, Räume für die technische Infrastruktur) sowie der betrachteten IT-Systeme
 - Vorhandene Sicherheitsmaßnahmen und Risiken für die betrachteten IT-Prozesse
4. *Festlegung der IT-Grundschutzmaßnahmen:* Für alle untersuchten IT-Systeme und Prozesse mit gängigen Risiko werden pauschal Maßnahmenempfehlungen festgelegt.
5. *Zusätzliche Maßnahmen für Systeme mit höherem Risiko:* Für alle Systeme und Prozesse, die der Gruppe mit höherem Risiko zuzuordnen sind, sollte zusätzlich eine detaillierte Sicherheitsanalyse durchgeführt werden. Diese muss sowohl Schwachstellenanalyse als auch eine individuelle Risikoanalyse gemäß dem IT-Sicherheitskonzept des BSI umfassen.

Risikoanalyse als Basis für Grundschutzmaßnahmen

Die Risikoanalyse liefert für ausgewählte IT-Systeme und IT-Prozesse auf der Basis der Ergebnisse von Bedrohungs- und Schwachstellenanalysen die Wahrscheinlichkeit für das Eintreffen eines gefährdenden Ereignisses und den damit verbundenen potenziellen Schaden.

Der *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz* beschreibt ausführlich Methoden zur Durchführung zusätzlicher IT-Risikoanalysen (siehe hierzu Abschnitt 1.2.3).

Im Rahmen der Maßnahmenempfehlungen müssen eine Reihe von konkreten Festlegungen getroffen werden. Zu den typischen Maßnahmenbereichen gehören unter anderem die folgenden:

- ▮ Passwortrichtlinien (Komplexität, Länge, Historie, Gültigkeitsdauer u. Ä.)
- ▮ Sicherheitsrichtlinien für alle Rechnersysteme, die zur Sicherheitsklasse mit normalem Risiko gehören (physische Sicherheit, BIOS-Absicherung, lokale Sicherheitsrichtlinien, Zugriffsschutz für Systemordner u. Ä.)
- ▮ Regelungen für den Umgang mit E-Mail (Verschlüsselung, private E-Mail-nutzung, Funktionspostfächer usw.)
- ▮ Regelungen zur Internetnutzung (Möglichkeiten zum Herunterladen von Software, Freischaltung von Freemailern usw.)
- ▮ Zugriffsschutz für mobile Geräte
- ▮ Regelungen für den Umgang mit USB-Schnittstellen (blockiert, kontrollierte Freigabe) und mit Wechseldatenträgern
- ▮ Richtlinien für die WLAN-Nutzung
- ▮ Umgang mit anderen drahtlosen Schnittstellen [BSI]

hinweis

Ein Sicherheitskonzept enthält in der Regel vertraulich zu behandelnde Informationen, die nicht beliebig weitergegeben werden dürfen. Hierzu können zum Beispiel Informationen über noch nicht beseitigte Schwachstellen zählen. Es sollte deshalb bereits bei der Erstellung darauf geachtet werden, dass es möglich ist, für die unterschiedlichen Zielgruppen die für sie relevanten Teile ausgliedern zu können. Eine entsprechende Gliederung des IT-Sicherheitskonzepts kann dies unterstützen.

Weitere Informationen zum hier vorgestellten IT-Grundschutz sind in der zahlreichen Literatur zum IT-Sicherheitskonzept zu finden. Eine der wichtigsten Informationsquellen stellt hier sicherlich das BSI dar. Hervorzuheben ist der *BSI-Standard 100-1 – Managementsysteme für Informationssicherheit (ISMS)* sowie Kapitel 4 des *BSI-Standards 100-2 - IT-Grundschutz-Vorgehensweise*. Diese beiden Schriften liefern eine detaillierte Anleitung zur Erstellung einer IT-Sicherheitskonzeption gemäß IT-Grundschutz.

hinweis

Mit dem Tool IT-Grundschutz (GSTOOL) stellt das BSI außerdem eine Software bereit, die den Anwender bei der Erstellung, Verwaltung und Fortbeschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz nach den BSI-Standards 100-1 bis 100-3 unterstützt.

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen für die aktuelle Version von GSTOOL finden Sie im Steckbrief in Anhang D.1.

Eine gute Informationssammlung mit einer Musterdokumentation für ein IT-Sicherheitskonzept findet sich weiterhin im Infoportal des Landesdatenbeauftragten für Datenschutz und Informationsfreiheit Saarland [LFDI].

3.2.3.2 Zusammenspiel mit dem Notfallhandbuch

Aufgabe des IT-Sicherheitskonzepts ist es auch zu regeln, wie mit vertraulichen Daten wie Administrator-Passwörtern oder Lizenzschlüsseln umgegangen werden soll. Derartige Regelungen, die auch für den Notfall relevant sind, sollten herausgehoben betrachtet werden.

Ohne Passwörter geht im Notfall gar nichts

Eigentlich hört es sich trivial an, trotzdem muss es erwähnt werden: Bei einem Notfall müssen alle erforderlichen Informationen verfügbar sein. Hierzu zählen insbesondere auch Lizenzschlüssel und Administrator-Passwörter. So ist beispielsweise für die Autorisierung eines DHCP-Servers in Active Directory die Berechtigung eines Organisations-Administrators erforderlich. Ist dieser „wichtige Mensch“ bei einem Notfall nicht erreichbar und das Kennwort nicht verfügbar, stellt dies ein ernsthaftes Problem dar. Gleiches gilt, wenn beispielsweise ein externer Mitarbeiter im Notfall die Active Directory-Datenbank zurücksichern soll, aber nicht autorisiert ist.

Da derartige Informationen nicht ausschließlich im Notfall verfügbar sein müssen, da sie gegebenenfalls auch bei normalen Änderungsprozessen benötigt werden, ist es nicht sinnvoll, die damit verbundenen Regelungen ausschließlich im Notfallhandbuch zu definieren. Besser ist es diese Informationen im IT-Sicherheitskonzept zu pflegen und in das Notfallhandbuch als Verweis bzw. in Kopie aufzunehmen.

3.2.4 IT-Risikohandbuch

» Für *IT-Risikohandbuch* synonym verwendete Begriffe: Risikohandbuch, Risikoplan «

Ein unternehmensweites Risikohandbuch bildet die Grundlage eines unternehmensweiten Risikomanagements. Es stellt organisatorische Maßnahmen und Regelungen dar, die zur Risikoerkennung, -quantifizierung, -kommunikation, -steuerung und Risikokontrolle 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 1.1.2.1) 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 aber ein Problem mit der Abgrenzung zum IT-Sicherheitshandbuch. Weil nämlich Riskohandbücher in der Vergangenheit die Risiken, die sich aus dem IT-Betrieb ergaben, nicht berücksichtigten, hat das BSI die Risikoanalyse als Ergänzung des IT-Grundschutz-Sicherheitskonzepts in seine Bausteine aufgenommen. Gemäß der obigen Beschreibung fordert aber auch das IT-Risikohandbuch entsprechende Risikoanalysen und Maßnahmenkataloge.

Schwierige
Abgrenzung
zum IT-Sicher-
heitskonzept

Wie bereits mehrfach betont, bleibt an dieser Stelle nur eine klare Definition und Abgrenzung der jeweils im Unternehmen benötigten Dokumente. So kann beispielsweise das IT-Risikohandbuch als strategisches Dokument definiert werden, das auf einem abstrakten Level das Risikomanagement regelt, während das IT-Sicherheitskonzept einen konkreten Maßnahmenkatalog auf der Grundlage einer Risikoanalyse liefert, die gemäß BSI-Standard erstellt wurde. Alternativ kann auch das IT-Risikohandbuch einen Risikoplan mit allen ermittelten Risiken enthalten, während das IT-Sicherheitskonzept systematische Gegenmaßnahmen beschreibt.

Da die Gewährleistung der IT-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.

Regelmäßige
Überprüfung

Business Impact-Analyse ist Basis für Risikohandbuch

Mit der zunehmenden Ausrichtung der Unternehmen an Prozessen gewinnt auch die *Business Impact-Analyse (BIA)* zunehmend an Bedeutung. Auch das Risikohandbuch sollte auf einer BIA aufbauen. Was aber verbirgt sich hinter einer die „Auswirkungsanalyse“, d. h. einer BIA. Business Impact-Analyse ist eine Methode des *Business Continuity Managements (BCM)* und dient der Identifizierung und Erfassung von Prozessen innerhalb eines Unternehmens. Ziel ist es, wechselseitige Abhängigkeiten zwischen den Prozessen und/oder den Unternehmensbereichen aufzuzeigen und die Auswirkungen bei Ausfall von Prozessen bzw. die benötigten Wiederanlaufzeiten zu ermitteln.

Zusammen mit der Risikoanalyse bildet die BIA die Grundlage für eine Sicherheits- und Notfallstrategie und die Basis für das Notfallkonzept bzw. das Notfallhandbuch. Einige weitere Erläuterungen zur Business Impact-Analyse finden Sie in Abschnitt 5.1.3.1.

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.

3.2.5 IT-Notfallkonzept



Für *Notfallkonzept* synonym verwendete Begriffe:
Notfallhandbuch



In den vorstehenden Abschnitten wurde mehrfach auf das Notfallkonzept verwiesen. Hierbei handelt es sich um ein Dokument, das die *Notfallvorsorge* im Blickpunkt hat. Damit grenzt es sich vom Notfallhandbuch ab, dessen Aufgabenschwerpunkt die Notfallbewältigung ist.

Als übergeordnetes Regelwerk sollte es den Rahmendokumenten zugeordnet werden. Es beschreibt die Strategien und Vorgaben für alle Aktivitäten der Notfallbewältigung. Alle Maßnahmen und Tätigkeiten, die hingegen zur eigentlichen Bewältigung eines Notfalls beitragen, sind im Notfallhandbuch zu beschreiben.

Inhalt des
Notfallkonzepts

Was genau im Notfallkonzept geregelt wird, obliegt dem Unternehmen und ist von diesem festzulegen. Möglicherweise gibt es ein unternehmensweites Notfallkonzept, das lediglich durch ein separates IT-Notfallkonzept ergänzt werden muss.

Eine nähere Betrachtung des Notfallkonzepts erfolgt in Kapitel 5, „Dokumentation für den Notfall“.

3.2.6 IT-Verfahrensverzeichnis

Das Bundesdatenschutzgesetz (BDSG) definiert verbindlich für alle Unternehmen, die der gesetzlichen Meldepflicht unterliegen, klare Anforderungen bezüglich der Einhaltung des Datenschutzes und der Datensicherheit. Zur Einhaltung eines gesetzeskonformen Datenschutzmanagements ist unter anderem die Pflege eines sogenannten *Verfahrensverzeichnisses* durch den Datenschutzbeauftragten des Unternehmens für alle Unternehmen vorgeschrieben,

Das Verfahrensverzeichnis muss alle automatisierten Verfahren einer Organisation auflisten, mit denen im Rahmen eines automatisierten Verfahrens ermittelte personenbezogene Daten gespeichert werden.

Definition
Verfahren

Der Begriff *Verfahren* wird vorrangig im datenschutzrechtlichen Zusammenhang verwendet und bezeichnet hier Vorgänge, in denen personenbezogene Daten verarbeitet oder genutzt werden. Ein typisches Verfahren ist eine automatisierte Zeiterfassung. Die für ein Verfahren verantwortliche Stelle muss im Verfahrensverzeichnis Angaben zu sämtlichen von ihr betriebenen automatisierten Verfahren machen, mit denen sie personenbezogene Daten verarbeitet.

Entsprechend der Zielsetzung des Verfahrensverzeichnisses konzentriert sich sein Inhalt auf die Offenlegung der für die Verarbeitung personenbezogener Daten verantwortlichen Stellen und Personen, auf die Zweckbestimmung der Verarbeitung sowie auf die betroffenen Personengruppen. Außerdem müssen Regelfristen für die Datenlöschung definiert werden. Konkret schreibt das BDSG vor, dass der für den Datenschutz Zuständige in geeigneter Weise gemäß § 4e Abs. 1 die folgenden Angaben für alle Betroffenen verfügbar zu machen hat.

„Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.“

tipp

Es gibt im Internet eine ganze Reihe von Musterdokumentationen, die bei der Erstellung der Dokumente für das Verfahrensverzeichnis hilfreich sein können. Hervorzuheben ist die Publikation *Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG – Ein Praxisleitfaden*, die vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) bereitgestellt wird. Das Dokument liefert neben einer umfassenden Übersicht, einem Beispiel eines Verfahrensverzeichnisses und diversen Formularen auch Beispiele für Programme zur Erstellung des Verfahrensverzeichnisses [BITKOM].

3.2.7 IT-Rollenkonzept

» Für *Rollenkonzept* synonym verwendete Begriffe: Rollenmodell, Berechtigungskonzept



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

Was ist eine Rolle?

Ein *Beispiel* ist die Rolle „Support-Mitarbeiter“: Ein Mitarbeiter, der diese Rolle innehat, soll bestimmte Aufgaben erfüllen und benötigt bestimmte Rechte und Befugnisse, um seine Aufgaben erfüllen zu können. So ist der Inhaber dieser Rolle beispielsweise befugt, Störungen anzunehmen und Störungsmeldungen im Ticket-System einzutragen. In der Beschreibung der Rolle muss also genau festgelegt sein, was ein Support-Mitarbeiter überhaupt ist, welche Tätigkeiten er auszuführen hat, welche Befugnisse er hat und welche fachlichen und persönlichen Fähigkeiten für die Ausübung der Rolle erforderlich sind. In der Prozessbeschreibung für die Annahme und Abwicklung von Störungen wiederum steht als Bearbeiter nicht der Mitarbeiter XY, sondern die Rolle „Support-Mitarbeiter“. Dies gewährleistet die Unabhängigkeit von organisatorischen und projektspezifischen Rahmenbedingungen.

Aufgabe des
Rollenkonzepts

Das Rollenkonzept definiert und beschreibt alle im Bereich der IT eingesetzten Rollen. Mit Hilfe dieser Rollenbeschreibungen können in der Betriebsmatrix die Mitarbeiter bzw. die Organisationseinheiten den Rollen zugeordnet werden. Wechselt beispielsweise ein Mitarbeiter des Backup-Teams in eine andere Abteilung, wird ihm lediglich die Rolle „Backup-Operator“ entzogen. Entsprechend seiner neuen Rolle in der neuen Abteilung können dem Mitarbeiter anhand des Rollenkonzepts alle erforderlichen Kompetenzen und Berechtigungen zugewiesen werden, ohne dass eine Änderung der Prozessdokumentation erforderlich ist. Lediglich die IT-Betriebsmatrix muss angepasst werden. Erläuterungen zur Erstellung einer IT-Betriebsmatrix finden Sie im nachfolgenden Abschnitt.

Die Zielgruppe für das Rollenkonzept sind die Organisationsverantwortlichen sowie die für das Personalmanagement verantwortlichen Mitarbeiter. Zwar müssen jedem Mitarbeiter die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein, doch ist dies eine Aufgabe der Prozessbeschreibungen und nicht des Rollenkonzepts. Entsprechend der Zielgruppe sind die Rollen abstrakt zu beschreiben.

hinweis

Ein Beispiel für eine Rollenbeschreibung finden Sie in Abschnitt 8.1.

Vorgaben
bei ITIL

Für die Standardprozesse, wie beispielsweise die Support-Prozesse, lohnt ein Blick auf das Rollenmodell von ITIL, da für diese Prozesse bereits zahlreiche Dokumentationen vorliegen, von denen vielfach zumindest Teile in die eigene Dokumentation übernommen werden können. Die in ITIL beschriebenen Prozesse definieren jeweils einen Prozesseigner, der die Zielvorgaben und die Kontrolle des Prozesses verantwortet, einen Prozess-Manager, der für die Umsetzung des Prozesses verantwortlich ist, und einen oder mehrere Servicetechniker für die operative Umsetzung des Prozesses.

3.2.8 IT-Betriebsmatrix

» Für *Betriebsmatrix* synonym verwendete Begriffe:
Betriebsorganigramm.



Wie im vorstehenden Kapitel beschrieben, werden beim prozessorientierten Ansatz Rollen definiert, denen Aufgaben und Verantwortlichkeiten zugewiesen werden.

Darüber hinaus muss es ein Dokument geben, in dem die Zuordnung von Organisationseinheiten und Personen zu den Rollen erfolgt, also ein Dokument, in dem konkret steht, welcher Rolle der Mitarbeiter XY zugeordnet ist. Dies ist die Aufgabe der sogenannten *Betriebsmatrix*. Diese definiert die organisatorische Platzierung der Aufgaben und Rollen. Dabei kann eine Person mehrere Rollen besetzen; ebenso kann aber auch eine Rolle von mehreren Personen eingenommen werden.

Eine Betriebsmatrix ermöglicht demzufolge eine eindeutige Zuordnung von Personen und Rollen und hilft dabei, Doppelbesetzungen, unklare Zuständigkeiten und Überschneidungen zu verhindern. Zeigt sich beispielsweise bei der Erstellung, dass ein Mitarbeiter Rollenträger für sehr viele Rollen ist, sollte überprüft werden, ob nicht einzelne Rollen auf andere Mitarbeiter übertragen werden können. Zwar ist es durchaus üblich, dass ein Mitarbeiter mehrere Rollen ausübt, doch wenn dieser Rolleninhaber dreier Rollen ist, die eigentlich jeweils 100 Prozent seiner Arbeitszeit beanspruchen, so stimmt etwas nicht. Möglicherweise wird dabei aber auch deutlich, dass wichtige Rollen überhaupt nicht eindeutig zugeordnet sind und im operativen Betrieb „irgendwie von irgendjemanden“ erledigt werden.

Vorteile einer
Betriebsmatrix

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

hinweis

Das Beispiel in Abschnitt 8.2 zeigt an einem Auszug, wie eine solche Betriebsmatrix für den IT-Betrieb aussehen kann.

3.2.9 IT-Gruppenkonzept

» Für *Gruppenkonzept* synonym verwendete Begriffe:
Berechtigungskonzept, Administrationskonzept.



Wie in den vorstehenden Kapiteln ausgeführt wurde, werden alle für die Prozesse erforderlichen Rollen im Rollenkonzept definiert. Hierbei handelt es sich um eine rein organisatorische Zuordnung, in der keine systemtechnischen Zuordnungen festgelegt werden. Zusätzlich gibt es mit der Betriebsmatrix ein Dokument, in dem die Zuordnung von Organisationseinheiten und Personen zu den Rollen erfolgt.

Zuordnung einer Rolle zu einer Systemgruppe

Damit ist aber noch nicht festgelegt, wie Rollen systemtechnisch umzusetzen sind. Hierfür wird ein weiteres Dokument benötigt, das im vorliegenden Buch als IT-Gruppenkonzept bezeichnet wird. Dieses bildet im Hinblick auf die Benutzerverwaltung eine Schnittstelle zwischen der Prozessdokumentation und der Systemdokumentation, indem es alle systemtechnischen Gruppen aufführt, erläutert und eine Zuordnung zu den Rollen festschreibt.

Beispielsweise kann im Gruppenkonzept eine Active Directory-Sicherheitsgruppe „Helpdesk“ zu finden sein. Für diese Gruppe werden hier die systemseitigen Rechte definiert (beispielsweise Zugriffsberechtigungen für das Ticket-System). Weiter wird definiert, dass jeder Mitarbeiter, der die Rolle Support-Mitarbeiter inne hat, der Gruppe Active Directory-Gruppe „Helpdesk“ hinzuzufügen ist.

hinweis

Nicht in jedem Fall ist die Erstellung eines eigenständigen IT-Gruppenkonzepts erforderlich. Während in großen Unternehmen, die erfahrungsgemäß große Anzahl an Gruppen ein eigenständiges Dokument rechtfertigt, ist es unter Umständen auch möglich, die Zuordnung von Rollen zu Gruppen in einer Tabelle dem Rollenkonzept hinzuzufügen.

3.2.10 IT-Namenskonventionen

Auf den ersten Blick mögen Namenskonventionen zweitrangig erscheinen, jedoch sind sie in größeren Unternehmen unverzichtbar. 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 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.

Namenskonvention für eine Active Directory-Umgebung

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

- ▶ Server (ausgenommen Cluster-Systeme)
- ▶ Cluster-Systeme (virtuelle Server und Clusterknoten)
- ▶ Linux-/UNIX-Server
- ▶ Clients
- ▶ Domänen (ROOT-Domäne und Sub-Domänen)
- ▶ Standorte im Active Directory (Standorte, Standort-Links und Standort-eigenschaften)
- ▶ 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 Exchange (Exchange Server-Name, Routing Group, Connectoren, öffentliche Ordner, Verteilerlisten, persönliche Postfächer, Postfach-Alias, Funktions-Postfächer)

Sind für die Produktionsumgebung und die Testumgebung unterschiedliche Namensrichtlinien 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 auch für Dokumente verbindliche Namensregeln (sowohl Dokumententitel als auch Dateinamen) festgelegt werden. Im Rahmen der IT-Dokumentation nehmen Namenskonventionen einen hohen Stellenwert ein, da sie Auswirkungen auf alle anderen Dokumente haben.

Konventionen
auch für
Dokumente

3.2.11 IT-Projektmanagement-Handbuch

Das IT-Projektmanagement-Handbuch (PM-Handbuch) regelt die verbindlichen Sollvorgaben, die für alle IT-Einzelprojekte gelten. Aufgrund des übergeordneten Charakters wird es den Rahmendokumenten zugeordnet. Da eine inhaltliche Betrachtung des IT-Projektmanagement-Handbuches jedoch besser in Kapitel 6, „Dokumentation von IT-Projekten“, passt, sei an dieser Stelle lediglich auf das genannte Kapitel verwiesen.

3.2.12 IT-Dokumentationsrichtlinie

Mit wachsender Unternehmensgröße wird die Erstellung und Durchsetzung einer Dokumentationsrichtlinie zunehmend wichtiger. Diese wird sinnvollerweise übergeordnet auf Unternehmensebene definiert. Wo eine solche übergeordnete Richtlinie fehlt, sollte sie zumindest für die Ebene der IT-Dokumentation entwickelt werden.

Die Aufgabe einer Dokumentationsrichtlinie ist es, verbindliche Regelungen für den formalen Aufbau einzelner Dokumente festzulegen sowie verbindliche Dokumentationsprozesse zu definieren. Zum Inhalt einer solchen Richtlinie sollten die folgenden Punkte zählen:

- ▶ Richtlinien und Klassifizierungen, die für alle Dokumente gelten (Namenskonventionen, Bearbeitungsstatus, Nummerierungssystem u. Ä.)
- ▶ Formaler Aufbau der Einzeldokumente
- ▶ Dokumentationsprozesse (Freigabeprozesse, Beauftragungsprozesse, Review-Verfahren usw.)
- ▶ Regelungen zur Speicherung der Dokumente im Dateisystem bzw. im Dokumentenmanagement-System

Eine ausführliche Beschreibung der möglichen Inhalte einer Dokumentationsrichtlinie unter Berücksichtigung der genannten vier Punkte erfolgt in Abschnitt 7.1.

3.2.13 Rahmendokumente und ihre Abhängigkeiten

Die einzelnen Rahmendokumente können, wie bereits dargestellt wurde, nicht isoliert betrachtet werden, sondern stehen miteinander in Beziehung. Einen Ausschnitt aus diesen Beziehungen zeigt die nachstehende Grafik.

Ein weiteres Beispiel (Abhängigkeiten der Sicherheitsdokumente) finden Sie in Abschnitt 5.1.3.2.

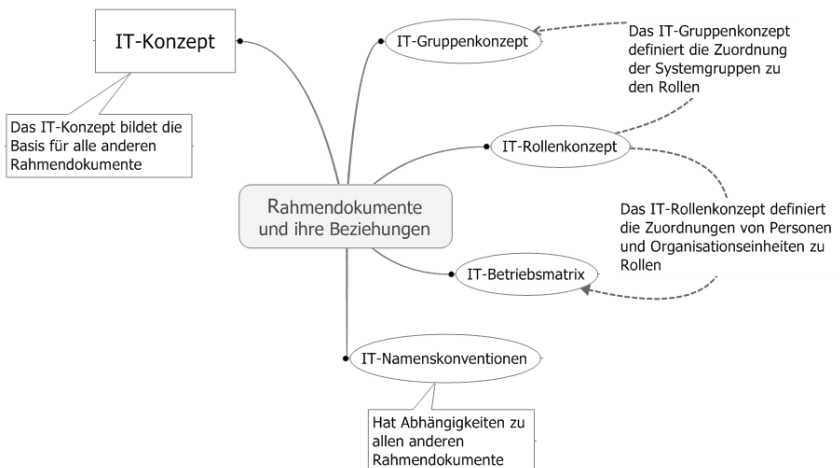


Abbildung 3.2: Rahmendokumente der IT-Dokumentation und ihre Abhängigkeiten: ein Ausschnitt

3.3 Fazit

Wie in diesem Kapitel gezeigt wurde, gibt es eine Reihe von Dokumenten, die übergeordneten Charakter haben und einen Rahmen für die Dokumente der drei Bereiche der IT-Dokumentation darstellen. Sie werden daher im vorliegenden Buch als Rahmendokumente bezeichnet.

Alle vorgestellten Dokumente können sowohl auf der Ebene der IT-Dokumentation als auch auf Unternehmensebene verwaltet werden. So ist es beispielsweise möglich und auch üblich, ein unternehmensweites Risikohandbuch zu führen und die IT-Service gefährdenden Risiken in einem gesonderten IT-Risikohandbuch im Rahmen der IT-Dokumentation zu pflegen.

Welche IT-Rahmendokumente also im individuellen Fall zu erstellen sind, hängt weitgehend davon ab, ob und mit welcher Ausprägung unternehmensweit gültige Dokumente existieren. Im Idealfall gibt es übergeordnete Unternehmensdokumente, die auf einem hohen Abstraktionsniveau allgemeingültige Richtlinien enthalten. Diese werden durch detaillierte Vorgaben in den entsprechenden Dokumenten der Organisationseinheiten ergänzt.