



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

IT-Grundschutz-konforme Dokumentation

FAQ und Einführung



Änderungshistorie

Version	Datum	Beschreibung
Community Draft 1.0	17.06.2024	Erster öffentlicher Entwurf IT-Grundschutz-konforme Dokumentation (FAQ und Hilfsmittel zur Dokumentation im IT-Grundschutz Stand Kompendium 2023). Es wird um Kommentierung und Rückmeldung gebeten. Dies kann an IT-Grundschutz@bsi.bund.de gerichtet werden.

Tabelle 1: Änderungshistorie

Vorwort

Das Thema Dokumentation wird bisher im IT-Grundschutz an verschiedensten Stellen behandelt. Angefangen, bei den BSI-Standards 200-1 bis 3 über die Referenzdokumente, bis hin zum IT-Grundschutz-Kompendium finden sich Informationen und Anforderungen, inhaltlicher und organisatorischer Natur an die Dokumentation im IT-Grundschutz.

Dieses Dokument soll in Ergänzung mit der *Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023* einen zentralen Einstiegspunkt zur Dokumentation bieten. Das vorliegende Dokument führt durch alle relevanten Aspekte hinsichtlich Dokumentation und verweist auf die weiterführende Information in den entsprechenden weiteren IT-Grundschutz Veröffentlichungen.

Dieses Dokument und die zugehörige *Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023* sind nicht normativ in der Umsetzung. Sie sind viel eher als eine Empfehlung zu verstehen und helfen dabei, die normativen Veröffentlichungen (insbesondere die BSI-Standards und das IT-Grundschutz-Kompendium) hinsichtlich Dokumentationen zu interpretieren und eine vom BSI vorgeschlagene Dokumentenstruktur aufzubauen.

Perspektivisch sollen die Inhalte direkt in die grundlegenden IT-Grundschutz-Veröffentlichungen eingepflegt werden, d. h. in die BSI-Standards und das IT-Grundschutz-Kompendium, sowie an allen anderen Stellen, wo Dokumentationen verbindlich gefordert werden. Es ist daher empfehlenswert, die eigene Dokumentation an dieser Veröffentlichung zu orientieren. Es wird jedoch auch perspektivisch erheblichen Freiraum in der Umsetzung der Dokumentation bzw. der damit verbundenen Struktur geben, da es in der Natur der Sache liegt, dass je nach Institutionsgröße, Branche oder auch Institutionskultur, eine andere Dokumentationsstruktur am besten geeignet ist.

Inhalt

1	Einleitung.....	5
2	Welche Typen von Dokumentationsaufwänden gibt es?	6
3	Wer oder was erstellt typischerweise die Dokumentationsaufwände eines Typs?.....	10
3.1	Autoren von: Strategischen Dokumentationsaufwänden	10
3.2	Autoren von: Taktischen Dokumentationsaufwänden	10
3.3	Autoren von: Operativen DA - Gestaltung.....	10
3.4	Autoren von: Operativen DA - Vermittlung.....	11
3.5	Autoren und Quellen von: Operativen DA - Ergebnis.....	11
4	In welchen Fällen sind welche Dokumentationen erforderlich?	12
5	Welche Dokumentationen sind notwendig für eine Konformität zu ISO 27001?	15
6	Welche Eigenschaften werden von den erforderlichen Dokumentationsaufwänden erwartet?	16
7	Auf welche Eigenschaften können die erforderlichen Dokumentationen verzichten?	18
8	Welche Hilfsmittel gibt es zur Erstellung der erforderlichen Dokumentationen?	19
9	Wann können an sich erforderliche Dokumentationen entbehrlich sein?	20
10	Wie werden Begriffe im Zusammenhang der Dokumentationsaufwände verstanden?.....	21
11	Wo finden sich die Dokumente und Materialien des BSI?	23

1 Einleitung

Ein zentraler Bestandteil der Informationssicherheit ist neben vielen anderen Themen die Dokumentation. Denn nur mit einer guten Dokumentation können Prozesse standardisiert und reproduziert, Informationen ausgetauscht und weitergegeben, sowie Beweise und Daten gesichert werden. Ferner dient Dokumentation dazu, verbindliche Vorgaben zu etablieren, Konformität nachzuweisen sowie getroffene Entscheidungen nachvollziehbar zu machen, um nur einige Beispiele zu nennen.

Daher erfordert die Umsetzung des IT-Grundschutzes in einem Informationsverbund verschiedene Dokumentationsaufwände (DAs). Dies können z. B. Dokumente zur Vermittlung von Inhalten an die Mitarbeitenden innerhalb der Institution sein oder Dokumente, die sich aus der Erfüllung von Anforderungen als Ergebnisdokumente im Informationsverbund ergeben oder erforderliche Dokumentationen zur Erlangung eines Zertifikats nach ISO 27001 auf der Basis von IT-Grundschutz.

Mit dem Begriff Dokumentationsaufwand sind sämtliche zu dokumentierende Informationen gemeint. Diese können in unterschiedlichster Form vorliegen z. B. als Word-Dokument, als Konfigurationsdatei, als Logdatei, als handschriftliches Protokoll, Wiki-Eintrag oder als Export eines IT-Grundschutz-Tools. Die Dokumentationsaufwände müssen und werden in aller Regel nicht immer manuell erstellt. Auch automatisiert erstellte Informationen sind als Dokumentation geeignet. Ein Beispiel hierfür sind Logdateien, die durch eine Anwendung oder durch einen Export eines IT-Grundschutz-Tools zur Schutzbedarfsfeststellung mit automatisch vererbten Schutzbedarfen erzeugt werden.

Ohne die Erstellung oder das Vorhandensein der jeweils erforderlichen Dokumentationen ist ein modellierter Baustein regelmäßig nicht vollständig umgesetzt. In der Folge können die Reife für ein Testat nach der Basisabsicherung oder ein Zertifikat nach ISO27001 auf Basis von IT-Grundschutz gefährdet sein bzw. kann ein erheblicher Mangel vorliegen.

Das vorliegende Dokument ist die zentrale Übersicht und Erläuterung zur Dokumentation im IT-Grundschutz. Es ergänzt die aktuellen BSI-Standards 200-1 und 200-2, bis die hierin enthaltenen Inhalte in eine überarbeitete Fassung der Standards eingearbeitet wurden.

Im weiteren Verlauf werden folgende Fragen beantwortet:

- [Welche Typen von Dokumentationsaufwänden gibt es?](#)
- [Wer oder was erstellt typischerweise die Dokumentationsaufwände eines Typs?](#)
- [In welchen Fällen sind welche Dokumentationsaufwände erforderlich?](#)
- [Welche Dokumentationsaufwände sind notwendig für eine Konformität zu ISO 27001?](#)
- [Welche Eigenschaften werden von den erforderlichen Dokumentationsaufwänden erwartet?](#)
- [Auf welche Eigenschaften können die erforderlichen Dokumentationsaufwände verzichten?](#)
- [Welche Hilfsmittel gibt es zur Erstellung der erforderlichen Dokumentationsaufwände?](#)
- [Wann können an sich erforderliche Dokumentationsaufwände entbehrlich sein?](#)
- [Wie werden Begriffe im Zusammenhang der Dokumentationsaufwände verstanden?](#)
- [Wo finden sich die Dokumente und Materialien des BSI?](#)

2 Welche Typen von Dokumentationsaufwänden gibt es?

Die im Rahmen der Umsetzung des IT-Grundschutzes entstehenden Dokumentationsaufwände verfolgen unterschiedliche Ziele und Zwecke und sind für unterschiedliche Zielgruppen relevant. Hieraus ergibt sich die Möglichkeit einer thematischen Gliederung. Die nachfolgende Dokumentationspyramide zeigt auf, wie die verschiedenen Dokumentationsaufwände thematisch gegliedert werden können:

Dokumentenpyramide IT-Grundschutz

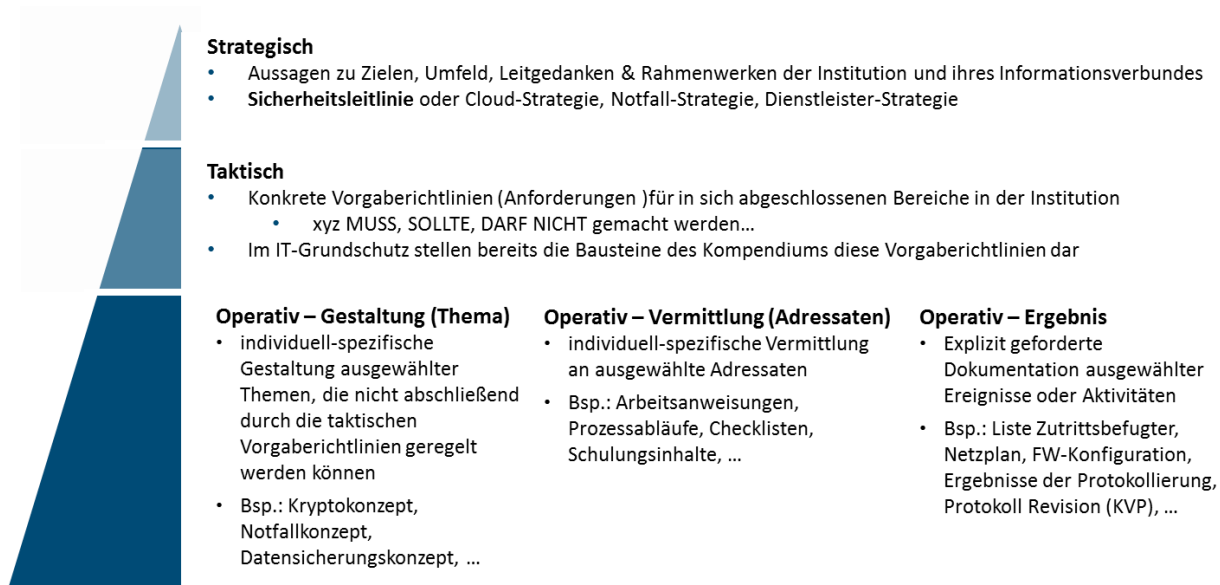


Abbildung 1: Dokumentationspyramide

Die Dokumentationspyramide ist ein häufig verwendetes Hilfsmittel, um die verschiedenen Dokumentationsstypen anhand ihrer Ordnungskriterien zu sortieren. Die wichtigen Unterschiede zwischen den Ebenen (strategisch, taktisch und operativ) sind Detailgrad, Änderungshäufigkeit und Zielgruppe.

Die nachfolgende Tabelle beschreibt die Dokumentationstypen im Detail und nennt Beispiele.

Typ	Beschreibung	Beispiele
Strategisch	Strategische Dokumente beinhalten Aussagen zu Umfeld, Zielen, Leitgedanken und Rahmenwerken des jeweiligen Informationsverbundes. Strategische Aussagen hinsichtlich des IT-Grundschutzes sind nur aus der Perspektive der Informationssicherheit erforderlich.	Leitlinie zur Informationssicherheit, Cloud-Strategie, Notfall-Strategie, Dienstleister-Strategie
Taktisch	Taktische Dokumentationen konkretisieren die strategischen Vorgaben z. B. aus der Leitlinie für die Informationssicherheit. Sie formulieren Anforderungen auf Abstraktionsniveau der Bausteine mittels Modalverben (MUSS, SOLLTE, DARF NICHT ...) und beschreiben somit, was zu tun ist. Taktische Dokumente umfassen organisatorische und personelle Sicherheitsaspekte aus allen relevanten Bereichen des ISMS, wie z. B.: • Sicherheitsaspekten betrieblicher Art • Detektion und Reaktion von/zu Sicherheitsvorfällen • Absicherung von Anwendungen, IT-Systemen, industrieller IT, Netzen und baulicher Infrastruktur Den Ausgangspunkt bilden die IT-Grundschutz-Bausteine des IT-Grundschutz-Kompodiums. D. h. die IT-Grundschutz-Bausteine des IT-Grundschutz-Kompodiums stellen bereits selbst die taktischen DAs dar. Ergänzungen und Konkretisierungen müssen durch die jeweilige Institution erfolgen (in der Regel durch den oder die ISB selbst). Änderungen an diesen Dokumenten können sich bspw. aufgrund der Ergebnisse aus der Modellierung oder der Risikoanalyse ergeben.	Vorhandene IT-Grundschutz-Bausteine des IT-Grundschutz-Kompodiums, aber auch benutzerdefinierte IT-Grundschutz-Bausteine können bereits als vollwertige taktische Dokumente verwendet werden oder als Vorlage dienen. Spezifische Anpassungen der IT-Grundschutz-Bausteine an die individuellen Gegebenheiten der Institution oder Ergänzungen z. B. zu höheren Schutzbedarfen, besonderen Einsatzumgebungen oder Komponenten, die durch die IT-Grundschutz-Bausteine nicht hinreichend abgedeckt sind.

Typ	Beschreibung	Beispiele
Operativ-Gestaltung	Operativ-gestalterische Dokumente greifen ausgewählte Aspekte der taktischen Dokumente auf. Sie beschreiben konkret für die jeweilige individuelle Institution und Anwendungsfall, wie die taktischen Vorgaben umgesetzt werden. Nicht für jedes taktische Dokument ist eine Konkretisierung und Beschreibung durch ein operativ-gestalterisches Dokument erforderlich.	Kryptokonzept, Notfallkonzept, Datensicherungskonzept, ...
Operativ-Vermittlung	Operativ-vermittelnde Dokumente greifen ausgewählte Aspekte der taktischen Dokumente auf. Sie vermitteln für die Mitarbeitenden der jeweiligen Institution, wie die taktischen Vorgaben umgesetzt werden sollen. Die operativ-vermittelnden Dokumente können dabei unterschiedliche Zielgruppen adressieren, z. B. richten sich die Schulungsunterlagen (IT-)Forensik speziell an die Mitarbeitenden der (IT-)Forensik. In einigen Fällen bietet es sich an, operativ-vermittelnde und operativ-gestalterische Dokumente in einem Dokument zusammenzufassen. Nicht für jedes taktische Dokument ist eine Vermittlung und Beschreibung durch ein operativ-vermittelndes Dokument erforderlich.	Arbeitsanweisungen, Prozessabläufe, Checklisten, Notfallpläne, Schulungsmedien, Benutzerhandbücher, ...
Operativ-Ergebnis	Die (Arbeits-)Ergebnisse aus der Umsetzung der taktischen und operativ-gestalterischen und -vermittelnden Dokumente werden in den operativ-Ergebnis-Dokumenten festgehalten. Nicht für jedes der vorgenannten Dokumente ist zwingend ein separates operatives-Ergebnis-Dokument zu erstellen. So ist z. B. für das Notfallhandbuch kein weitergehendes operativ-Ergebnis-Dokument zu erstellen. Das Notfallhandbuch selbst ist in diesem Fall bereits die hinreichende Dokumentation.	Liste Zutrittsbefugter, Bereinigter Netzplan, Ergebnisdokumentation Protokollierung, IV-Assets der Strukturanalyse, Auditberichte, Ergebnisse eines IT-Grundschutz-Checks, Schutzbedarfsfeststellungen ...

Tabelle 2: Beschreibung Dokumentationstypen

Die Dokumentenpyramide mit den Dokumentationstypen ist lediglich als Hilfsmittel zur Strukturierung und Gliederung der Dokumentationsaufwände in einer Institution zu verstehen. Aus der Dokumentenpyramide

werden keine formalen Anforderungen an die Dokumentationsaufwände abgeleitet. So kann ein Dokument Inhalte enthalten, die sich mehr als einem Typ zuordnen lassen. Dies gilt insbesondere für operative Dokumente, die sowohl Inhalte zu Gestaltung als auch zu Vermittlung und ggf. Ergebnissen enthalten können. Ein „Operativ-Ergebnis“-Dokument setzt z. B. nicht zwingend einen „Operativ-Vermittlung“ oder „Operativ-Gestaltung“-Dokument voraus. Dies bedeutet, es muss aus rein formalen Gründen kein operativ vermittelndes oder gestalterisches Dokument erstellt werden.

3 Wer oder was erstellt typischerweise die Dokumentationsaufwände eines Typs?

Die nachfolgenden Aussagen zu den Autoren und Quellen der Dokumentationsaufwände sind keine verbindlichen Vorgaben. Sie dienen der Orientierung und Erläuterung, welche Rollen in einer Institution typischerweise welche Dokumente erstellen.

3.1 Autoren von: Strategischen Dokumentationsaufwänden

Strategische Dokumentationsaufwände werden von der Leitungsebene verantwortet, initiiert und verabschiedet. Die Erstellung der Inhalte kann an den oder die Informationssicherheitsbeauftragte(n) (ISB) und das Informationssicherheitsmanagement-Team (ISM-Team) delegiert werden (oder ersatzweise an andere Personen mit dem erforderlichen Fachwissen).

ISB und ISM-Team erstellen einen strategischen Dokumentationsaufwand federführend selbst (in der Regel die Leitlinie zur Informationssicherheit) oder in Zusammenarbeit mit thematisch betroffenen Organisationseinheiten: z. B. mit der Organisationseinheit IT-Strategie zu Cloud-Strategie; mit der Organisationseinheit Einkauf zu Dienstleister-Strategie und mit dem Business-Continuity-Team zu Business-Continuity-Strategie.

3.2 Autoren von: Taktischen Dokumentationsaufwänden

Taktische Dokumentationsaufwände werden von dem ISB und seinem ISM-Team erstellt und freigegeben. Die betroffenen Organisationseinheiten sollten die Erstellung und Qualitätssicherung durch fachliche Expertise unterstützen und begleiten. So soll erreicht werden, dass die Anforderungen auch durch die Organisationseinheiten möglichst effizient und effektiv erfüllt werden können.

Den Ausgangspunkt für die taktischen Dokumentationsaufwände bilden die IT-Grundschatz-Bausteine (des IT-Grundschatz-Kompodiums und vom Anwendenden erstellte). Jeder modellierte IT-Grundschatz-Baustein kann bereits einen vollwertigen taktischen Dokumentationsaufwand zu dem jeweiligen Thema des Bausteins darstellen. Bei Bedarf können die IT-Grundschatz-Bausteine und damit die taktischen Dokumentationsaufwände für einen Informationsverbund (IV) konkretisiert oder ergänzt werden (s.o.): institutionsspezifische Anpassungen der IT-Grundschatz-Bausteine an die Gegebenheiten der Institution oder Ergänzungen z. B. zu höheren Schutzbedarfen, besonderen Einsatzumgebungen oder Komponenten, die durch die IT-Grundschatz-Bausteine nicht hinreichend abgedeckt sind.

3.3 Autoren von: Operativen DA - Gestaltung

Die Dokumentationsaufwände des Typs „Operativ – Gestaltung“ werden direkt von den thematisch betroffenen Organisationseinheiten und Mitarbeitenden (je nach Thema können dies auch ISB und ISM-Team sein) erstellt. Ihre Erstellung erfolgt maßgeblich durch die jeweilige Organisationseinheit, an die sich das jeweilige Dokument richtet.

Bei Bedarf kann die Erstellung durch Personen unterstützt werden, die sowohl ausreichend tief im jeweiligen Fachthema verankert sind (wie z. B. Netzdesign, SW-Entwicklung oder bauliche Infrastruktur) als auch über die entsprechenden Kompetenzen in der Informationssicherheit verfügen (speziell auch in den Rahmenwerken zur Informationssicherheit, die in der Institution zur Anwendung kommen sollen). Durch diese Zweigleisigkeit bilden diese Personen eine kommunikative und fachlich kompetente Schnittstelle zwischen einer Organisationseinheit und dem ISB mit dessen ISM-Team.

Die Dokumentationsaufwände des Typs „Operativ – Gestaltung“ sollten so geschrieben sein, dass die betroffenen Organisationseinheiten davon eigenständig Dokumentationen des Typs „Operativ – Vermittlung“ ableiten können, wenn Bedarf zu diesen besteht. Je weniger komplex ein Informationsverbund ist, desto eher kann es angemessen sein, gestaltende und vermittelnde Inhalte operativer Dokumente gleich in einem Dokument zu bündeln, etwa, weil sie sich an den selben Personenkreis richten.

3.4 Autoren von: Operativen DA - Vermittlung

Die Beschreibung zu den Autoren von „Operative DA – Gestaltung“ gilt auch hier.

3.5 Autoren und Quellen von: Operativen DA - Ergebnis

Die Ergebnisse der Umsetzung der taktischen und operativen Dokumentationen werden durch die jeweiligen Organisationseinheiten oder Fachexperten erstellt bzw. festgehalten. Je nach Dokumentationsaufwand kann die Erstellung der Ergebnis-Dokumente manuell oder automatisiert erfolgen. Letztere z. B. als Export einer Applikation oder Appliance, die die Quelle von Protokolldaten sein können.

Die vorgestellte Dokumentenstruktur ist dabei nur als eine Möglichkeit zur Umsetzung zu verstehen. Im Einzelfall kann es sinnvoll sein, hiervon abzuweichen. Hierzu werden an entsprechender Stelle im Hilfsmittel auch Hinweise gegeben.

[illegible]

- Im **Tabellenblatt „Basis-Absicherung“** werden alle geforderten Dokumentationsaufwände des BSI-Standards 200-2 im Falle einer Basis-Absicherung aufgeführt.
- Im **Tabellenblatt „Standard-Absicherung“** werden alle geforderten Dokumentationsaufwände des BSI-Standards 200-2 im Falle einer Standard-Absicherung aufgeführt.
- Im **Tabellenblatt „Baustein-Dach“** werden alle geforderten Dokumentationsaufwände aus dem IT-Grundschutz-Kompendium aufgeführt. In der Regel handelt es sich hierbei um Dachdokumente. D.h.

diese werden in der Regel durch unterschiedliche Bausteine der Prozess-Schicht begründet und durch unterschiedliche Bausteine der SYS-Schicht bei Bedarf, sofern relevant und modelliert, ergänzt. So finden sich in diesem Tabellenblatt einerseits die originären Anforderungen aus den Prozessbausteinen in der Spalte *übergreifende Themen*, die in der Regel immer erfüllt werden müssen, soweit die entsprechenden IT-Grundschutz-Bausteine modelliert wurden. Ergänzt wird dies in der Spalte *bausteinspezifische Ergänzungen* durch entsprechende Anforderungen der Bausteine der Schicht SYS.

Ergänzt werden diese Informationen durch eine Zuordnung zu den Stufen *Basis*, *Standard* oder *erhöhter Schutzbedarf*, die die Stufe der Anforderungen aus übergreifende Themen reflektiert.

Ferner werden die einzelnen Dach-Dokumente einem oder mehreren Typen aus der Dokumentpyramide zugeordnet. Werden mehrere Typen ausgewählt, so wird der führende Typ dick markiert.

- Im **Tabellenblatt Baustein-Verweise auf Dach** werden alle restlichen Bausteine des IT-Grundschutz-Kompendiums und deren Anforderungen an die Dokumentation aufgelistet, aus denen keine eigenen Dokumente hervorgehen (müssen). Diese Anforderungen/Aspekte hinsichtlich Dokumentationen können in den entsprechenden Dach-Dokumenten ergänzt werden. Eine entsprechende Zuordnung wird hier auch dargestellt und ist nur als nichtnormative Empfehlung zu verstehen:

Baustein	Anforderungen
OPS.1.2.6	Keine notwendigen DA-Inhalte des Bausteins.
APP.1.1	<u>Einrichtung</u> APP.1.1: A11 (→ OPS.1.1.6) <u>Benutzende</u> APP.1.1: A10, A13 (→ DA Infosec MA)
APP.1.2	Keine notwendigen DA-Inhalte des Bausteins.
APP.1.4	Keine notwendigen DA-Inhalte des Bausteins.
APP.2.1	<u>Planung</u> A9 → Anforderungskatalog (APP.6) <u>Betrieb</u> A1 → IT-Betriebskonzept (OPS.1.1.1) A1 → Sicherheitskonzept bzw. die Anforderungen des Bausteins APP.2.1 geben dabei bereits alle wesentlichen Inhalt des Bausteins der dokumentierten Umsetzung der Richtlinie entspricht. A2, A3 → Konzept zum Identitäts- und Berechtigungsmanagement (ORP.4) A2, A6, A15 → IT-Betriebskonzept (OPS.1.1.1) <u>Notfall</u> A16 → Notfallhandbuch (DER.4)
APP.2.2	<u>Betrieb</u> A1 → Konzept zum Identitäts- und Berechtigungsmanagement (ORP.4) A3 → IT-Betriebskonzept (OPS.1.1.1) <u>Notfall</u> A5 → Notfallhandbuch (DER.4)

Abbildung 3: Auszug aus dem Tabellenblatt Baustein-Verweis auf Dach

- Im **Tabellenblatt ISO27001 DA->IT-GS DA** werden alle explizit geforderten DAs aus der ISO27001 entsprechenden DAs des IT-Grundschutzes zugeordnet. So kann die Kompatibilität nachvollzogen werden.
- Im **Tabellenblatt Hinweise IT-Betriebskonzept** werden weitergehende Informationen zum IT-Betriebskonzept gegeben. Dies wird im Tabellenblatt *Baustein-Dach* als sehr umfangreiches Dach-Dokument genannt, in dem wesentliche Inhalte des IT-Betriebs dokumentiert werden. Dementsprechend wird es auch durch eine Vielzahl von SYS-Bausteinen ergänzt. Dabei kann es zielführend sein, die Themen weiter zu gruppieren, zum Beispiel entsprechend der vorgeschlagenen Phasen (s. Abbildung 3). Alternativ kann es auch zielführend sein, das Dokument in kleinere Dokumente aufzuteilen oder mit weiteren Konzepten zu konsolidieren. Das Tabellenblatt *Hinweise IT-Betriebskonzept* und die Anmerkungen in dem Tabellenblatt *Baustein-Dach* geben weitere Hinweise hierzu.

Ein wesentlicher Grundgedanke bei der Beschreibung der möglichen Strukturierung der Dokumentationsaufwände, insbesondere im Tabellenblatt *Baustein-Dach*, besteht darin, zusammenhängende Dokumentationsaufwände in einem übergeordneten Dokument zusammenzufassen.

Z. B. kann es sich anbieten, die Prozesse des IT-Betriebs, die Dokumentationen der Konfigurationen der vom IT-Betrieb administrierten IT-Systeme im IT-Betriebskonzept zusammenzufassen. Dies verhindert eine zu kleinteilige Dokumentation, die häufig zu Redundanzen oder Widersprüchen und Mehraufwand in der Pflege der Dokumente führt.

5 Welche Dokumentationen sind notwendig für eine Konformität zu ISO 27001?

Der IT-Grundschutz ist vollständig kompatibel mit der internationalen Norm ISO/IEC 27001 (kurz ISO 27001). Mit Blick auf die Dokumentation versteht sich der IT-Grundschutz hierbei als eine Konkretisierung oder auch Umsetzungsanleitung zur ISO 27001. Hieraus ergibt sich folgende Regel:

Notwendige Dokumentationsaufwände nach IT-Grundschutz = Mindestens notwendige Dokumentationsaufwände nach ISO27001 + X

Die mindestens notwendigen Dokumentationsaufwände nach ISO27001 und die entsprechenden Dokumentationsaufwände aus dem IT-Grundschutz können dem Hilfsmittel „Übersicht über konsolidierte DA im IT-Grundschutz“ auf dem Tabellenblatt „ISO27001 DA->IT-GS DA“ entnommen werden. Jeder nach ISO 27001 mindestens notwendige Dokumentationsaufwand ist auch nach IT-Grundschutz notwendig.

Welche Dokumentationsaufwände nach IT-Grundschutz notwendig sind, beantwortet obige Tabelle im Kapitel 4: „In welchen Fällen sind welche Dokumentationen erforderlich?“. Dies schließt die mindestens notwendigen Dokumentationsaufwände nach ISO 27001 ein. Die mit „X“ gekennzeichneten Dokumentationsaufwände bezeichnen die darüber hinaus notwendigen Dokumentationsaufwände. Diese wurden bereits vom BSI in Risikoanalysen ermittelt. Die Ergebnisse dieser Risikoanalysen sind die IT-Grundschutz-Bausteine, die eben die über die ISO 27001 hinausgehenden Dokumentationsaufwände fordern (gilt nur für den normalen Schutzbedarf).

Bei der Umsetzung der ISO 27001 muss sich der Anwendende das „X“ selbst im Rahmen von eigenen Risikoanalysen erschließen. Weitere Maßnahmen schlägt der Annex A zur ISO 27001 vor. In den Worten der ISO 27001:2022 Abschnitt 7.5.1 b):

The organization's information security management system shall include: [...] documented information determined by the organization as being necessary for the effectiveness of the information security management system.

Die ISO 27002 gibt Hinweise, welche Dokumentationsaufwände dazu gehören könnten. Die Hinweise bestehen insbesondere in den Indikatoren *topic-specific policy* und *should be documented*. Im Gegensatz zu IT-Grundschutz liegt es bei der Umsetzung der ISO 27001 in der Verantwortung der Anwendenden, diese Dokumentationsaufwände zu bestimmen.

6 Welche Eigenschaften werden von den erforderlichen Dokumentationsaufwänden erwartet?

Es ist erforderlich, bestimmte Dokumentationen zu erstellen, wenn die Anforderungen eines IT-Grundschutz-Bausteins erfüllt werden sollen oder eine Basis- oder Standard-Absicherung angestrebt wird. Die erforderlichen Dokumentationen müssen bestimmte Eigenschaften erfüllen. Dies betrifft primär die Frage, wie ein Dokument gelenkt werden muss. Mit Lenkung von Dokumenten ist auf der einen Seite gemeint, wer diese steuert (Freigabeprozess, Finalisierungsprozess). Auf der anderen Seite beschreibt es, welche Anforderungen an die Dokumente, insbesondere in Hinblick auf die Kennzeichnungen gestellt werden.

Hierbei kann zwischen **minimaler** und **vollständiger** Lenkung unterschieden werden:

Eine **minimale Lenkung** realisiert mindestens folgende Eigenschaften zu einem Dokumentationsaufwand:

- Es ist leicht erkennbar, ob die Dokumentation aktuell ist (Aktualität). Ohne entsprechende offensichtliche Eigenschaften der Dokumentation sollte dessen Aktualität berechtigt angenommen werden können.
- Die Dokumentation ist den Befugten zugänglich (Verfügbarkeit). Unbefugte haben keinen Zugang oder Zugriff (Vertraulichkeit).
- Die Dokumentation ist vor unbeabsichtigten Änderungen geschützt (Integrität).

Eine **vollumfängliche Lenkung** realisiert folgende Eigenschaften zu einer Dokumentation:

- Siehe hierzu BSI-Standard 200-2 Kap.5.2.3 Abschnitt "Mindestanforderung an die Kennzeichnung der Dokumente zum Sicherheitsmanagement".

Die nachfolgende Tabelle betrachtet die Fragestellung näher, welche Dokumente welche erwarteten Eigenschaften haben, sprich minimal oder vollständig gelenkt werden müssen:

DA des Anwendungsfalls	Erwartete Eigenschaften
Umsetzung modellierter IT-Grundschutz-Bausteine in Dach-Dokumenten	<u>Erwartete Inhalte</u> Die Umsetzung modellierter IT-Grundschutz-Bausteine meint insbesondere die Erfüllung der Basis- und Standard-Anforderungen eines Bausteins. Damit ist auch die Erstellung von Dokumenten verbunden. Die erwarteten Inhalte dieser Dokumente werden durch die Anforderungen bestimmt, die die jeweilige Dokumentation fordern (s. Tabellenblatt <i>Baustein-Dach</i> in dem Hilfsmittel <i>Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023</i>). <u>Erforderliche Lenkung</u> Die zur Erfüllung der Anforderungen eines Bausteins notwendigen strategischen und taktischen Dokumente des Tabellenblattes <i>Baustein-Dach</i> müssen vollumfänglich gelenkt werden. Alle anderen notwendigen Dokumentationen des Tabellenblattes <i>Baustein-Dach</i> können hingegen nur minimal gelenkt werden.

DA des Anwendungs-falls	Erwartete Eigenschaften
Umsetzung der Basis-Absicherung	<u>Erwartete Inhalte</u> Mit der Umsetzung der Basis-Absicherung ergeben sich Dokumentationsaufwände zum einen aus den Anforderungen der modellierten IT-Grundschutz-Bausteine, zum anderen aber auch aus dem BSI-Standard 200-2. Die über die aus den IT-Grundschutz-Bausteinen hinaus geforderten Dokumentationsaufwände können dem BSI-Standard 200-2 Kapitel 6 entnommen werden bzw. werden in dem Hilfsmittel <i>Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023</i> in dem Tabellenblatt <i>Basis-Absicherung</i> aufgeführt. Wenn eine Institution ein „Testat nach der Basis-Absicherung“ anstrebt, unterstützt das zugehörige Prüfschema bei der Identifikation der für den Auditor erforderlichen Dokumentationen. Der Prüfbericht wird vom Auditor erstellt. <u>Erforderliche Lenkung</u> Die „Leitlinie zur Informationssicherheit“ muss stets vollumfänglich von der Institutionsleitung gelenkt werden. Alle anderen notwendigen Dokumentationen können hingegen nur minimal gelenkt werden.
Umsetzung der Standard-Absicherung	<u>Erwartete Inhalte</u> Mit der Umsetzung der Standard-Absicherung¹ ergeben sich Dokumentationsaufwände, zum einen aus den Anforderungen der modellierten IT-Grundschutz-Bausteine, zum anderen aber auch aus dem BSI-Standard 200-2. Die über die aus den IT-Grundschutz-Bausteinen hinaus geforderten Dokumentationsaufwände sowie Referenzdokumente können dem BSI-Standard 200-2 Kapitel 7 (Kern-Absicherung) und 8 (Standard-Absicherung) entnommen werden bzw. werden in dem Hilfsmittel <i>Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023</i> in dem Tabellenblatt <i>Standard-Absicherung</i> aufgeführt. Wenn eine Institution ein „ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“ anstrebt, unterstützt das Zertifizierungsschema bei der Identifikation der für den Auditor erforderlichen Dokumentationen. Der Prüfbericht wird vom Auditor erstellt. <u>Notwendige weitere Merkmale</u> Die Referenzdokumente bzw. die Dokumente aus dem Hilfsmittel <i>Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023</i> in dem Tabellenblatt <i>Standard-Absicherung</i> sowie die strategischen und taktischen Dokumente des Tabellenblattes <i>Baustein-Dach</i> müssen vollumfänglich gelenkt werden. Alle anderen notwendigen Dokumentationen können hingegen nur minimal gelenkt werden.

Tabelle 3: geforderte Eigenschaften zu den geforderten Dokumentationen

¹ In diesem Dokument wird zur Vereinfachung nicht zwischen Kern- und Standard-Absicherung unterschieden. In diesem Dokument ist mit der Standard-Absicherung sowohl die Standard-Absicherung als auch die Kern-Absicherung gemeint.

7 Auf welche Eigenschaften können die erforderlichen Dokumentationen verzichten?

Neben den Inhalten und der Lenkung gibt es keine weiteren notwendigen Eigenschaften, welche die Dokumentationen erfüllen und aufweisen müssen. Daraus folgt u.a., Dokumentationen:

- müssen nicht zwingend in digitaler Form vorliegen. Es kann z. B. eine angemessene Lösung sein, Zutritte zu einem Server-Raum analog (papierbasiert) zu erfassen.
- müssen nicht in einem bestimmten Daten-Format vorliegen. Ein Office-Format ist nicht immer passend z. B. wenn eine Dokumentation ein Schulungsvideo oder ein Firewall-Regelsatz ist.
- können auch automatisch erzeugt werden. In der Regel betrifft den Dokumentationstyp Operativ-Ergebnis, wie z. B. Logdaten. Beispiele für teilautomatisiert erstellte Dokumentationen sind die Referenzdokumente als Export eines IT-Grundschutz-Tools, das z. B. automatisiert die geltenden Regeln zur Ableitung von Schutzbedarfen anwendet.
- müssen nicht zwingend eigenständige Dokumente sein. In weniger komplexen Institutionen oder Informationsverbünden könnten z. B. alle Dokumentationen, die an den IT-Betrieb gerichtet sind, in einem IT-Betriebskonzept zusammengefasst werden.
- müssen nicht Inhalte aus IT-Grundschutz-Bausteinen wiederholen.

8 Welche Hilfsmittel gibt es zur Erstellung der erforderlichen Dokumentationen?

Das BSI hat zur Orientierung exemplarische Dokumentationen zu dem fiktiven Informationsverbund der RECPLAST GmbH veröffentlicht. Zu diesen zählen Stand Frühjahr 2024 die Dokumente

- Festlegung des Geltungsbereichs,
- die Strukturanalyse,
- die Schutzbedarfsfeststellung,
- die Modellierung,
- der IT-Grundschutz-Check,
- die Risikoanalyse sowie
- die Sicherheitsleitlinie.

IT-Grundschutz-Tools können bei der Erstellung von Dokumentationen ein geeignetes Hilfsmittel sein. Bei der Entscheidung, ob hierfür ein entsprechendes Tool eingesetzt werden soll, ist vorab zu prüfen, ob das Tool die eigenen individuellen Anforderungen erfüllt. Bei der Prüfung könnte ferner berücksichtigt werden, ob das Tool ausreichend Hilfestellung bei der vom IT-Grundschutz geforderten Dokumentation bietet.

9 Wann können an sich erforderliche Dokumentationen entbehrlich sein?

Welche Dokumentationen erforderlich sind, beantwortet das Kapitel: „[In welchen Fällen sind welche Dokumentationen erforderlich?](#)“

Dokumentationen die sich auf eine Lebenszyklusphase beziehen (bspw. Planungsphase), die bereits abgeschlossen ist, können entbehrlich sein. Es gilt:

- Es kann auf jede Dokumentation verzichtet werden, die eine bereits abgeschlossene Lebenszyklusphase betrifft.
- Es gibt z. B. keine obligatorischen Dokumentationen zu Anforderungsanalysen einer Komponente X, wenn die Komponente X bereits im Einsatz ist, also die Planungsphase bereits abgeschlossen ist.
- Es müssen keine separaten, eigenen Richtlinien (taktische Dokumente) erstellt werden, wenn ein Baustein dies in einer eigenen Anforderung fordert, sofern der Baustein ohne Abweichungen modelliert werden kann. In diesem Fall ist der Baustein mitsamt seinen ganzen Anforderungen die Richtlinie selbst und die dokumentierte Umsetzung des Bausteins dokumentiert gleichzeitig auch die Umsetzung der Richtlinie. Entsprechende Anforderungen bzw. Konstellationen sind in dem Hilfsmittel *Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023* gekennzeichnet und erläutert.

Das Kriterium zur Entbehrlichkeit einer Dokumentation beschränkt nicht die Prüfentscheidung eines Auditors, ob bspw. eine Komponente über die geforderten Eigenschaften verfügt oder in der geforderten Weise im Informationsverbund eingesetzt wird.

10 Wie werden Begriffe im Zusammenhang der Dokumentationsaufwände verstanden?

Begriff	Erläuterung
Umsetzung der Basis-Absicherung	Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-Absicherung (BSI-Standard 200-2 Kap.6)
Umsetzung der modellierten IT-Grundschutz-Bausteine	Erfüllung der Anforderungen eines IT-Grundschutz-Bausteins aus dem IT-Grundschutz-Kompendium.
Dokumentationsaufwand/Dokumentationen (DA, abgekürzt)	Der Begriff Dokumentationsaufwand oder Dokumentation soll zum Ausdruck bringen, dass dessen Inhalte in unterschiedlichster Form vorliegen können und dürfen: als Word-Dokument, als Log-Datei, als Video-Datei, als Konfigurationsdatei, als Protokolldatei, als Datenbankeinträge, als handschriftliches Protokoll, als Wiki-Eintrag usw.
ISB	Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter
ISM-Team	Informationssicherheitsmanagement-Team: Personen im Team des ISB bzw. unter der fachlichen Führung des ISB zur Wahrnehmung von Aufgaben des Informationssicherheitsmanagement.
Institution/ Informationsverbund	Als Informationsverbund (nach BSI 200-2 Kap.3.3.4) gilt der gewählte Geltungsbereich zur Umsetzung von IT-Grundschutz und damit der Erstellung notwendiger Dokumentationen.
Lenkung, minimale	Eine minimale Lenkung realisiert mindestens folgende Eigenschaften zu einem Dokumentationsaufwand: - Es ist leicht erkennbar, ob die Dokumentation aktuell ist (Aktualität). Ohne entsprechende offensichtliche Eigenschaften der Dokumentation sollte dessen Aktualität berechtigt angenommen werden können. - Die Dokumentation ist den Befugten zugänglich (Verfügbarkeit). Unbefugte haben keinen Zugang oder Zugriff (Vertraulichkeit). - Die Dokumentation ist vor unbeabsichtigten Änderungen geschützt (Integrität). Alle notwendigen Dokumentationen müssen mindestens minimal gelenkt werden.
Lenkung, vollumfängliche	Eine vollumfängliche Lenkung realisiert folgende Eigenschaften zu einer Dokumentation: BSI-Standard 200-2 Kap.5.2.3 Abschnitt "Mindestanforderung an die Kennzeichnung der Dokumente zum Sicherheitsmanagement". Nur die Referenzdokumente müssen vollumfänglich gelenkt werden.
OE	Organisationseinheiten: Die Organisationseinheiten in einer Institution oder einem Informationsverbund (IV), die typischerweise Teil der Aufbauorganisation sind, wie z. B. Einkauf, Recht & Compliance, IT-Betrieb, IT Servicemanagement, Gebäudemanagement, ISB, ISM-Team, ...

Begriff	Erläuterung
Operative Sicherheit	Gemeint sind Personen, die sowohl ausreichend tief im jeweiligen Fachthema verankert sind (wie z.B. Netzdesign, SW-Entwicklung, Personal/HR, Einkauf oder bauliche Infrastruktur) als auch über Grundkompetenz in der Informationssicherheit verfügen (speziell auch den Rahmenwerken zur Informationssicherheit, die in der Institution zu Anwendung kommen sollen). Durch diese Zweigleisigkeit bildet die operative Sicherheit eine kommunikative und kompetente Schnittstelle zwischen einer Organisationseinheit und dem ISB mit dessen ISM-Team.
Referenzdokumente	Teil der notwendigen Dokumentationen, die die Ergebnisse der IT-Grundschutz-Vorgehensweise nach BSI-Standard 200-2 dokumentieren. Je nachdem ob die Basis-, Kern- oder Standard-Absicherung angestrebt wird, können dazu gehören: die Festlegung des Geltungsbereichs, die Strukturanalyse, die Schutzbedarfsfeststellung, die Modellierung, der IT-Grundschutz-Check, die Risikoanalyse und die Sicherheitsleitlinie. Können dem Hilfsmittel <i>Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023</i> den Tabellenblättern <i>Standard-Absicherung</i> und <i>Basis-Absicherung</i> entnommen werden.
Umsetzung der Standard-Absicherung	Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung (BSI-Standard 200-2 Kap.8).

Tabelle 4: Glossar

11 Wo finden sich die Dokumente und Materialien des BSI?

Gegenstand	Quelle
IT-Grundschutz-Bausteine	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html
BSI-Standard 200-1	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html
BSI-Standard 200-2	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html
BSI-Standard 200-3	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html
IT-Grundschutz-Tools	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/IT-Grundschutztools_node.html
Prüfschema	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Testat/Pruefschema.html
RECPLAST	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/recplast_node.html
Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Community_Draft/Uebersicht_DA-IT-Grundschutz_Kompendium_2023.html
Zertifizierungsschema	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/Zertifizierungsschema/schema_node.html

Tabelle 5: Quellenverzeichnis