



# Aktuelles und Diskussion zum IT-Grundschutz

Holger Schildt, Referatsleiter BSI-Standards und IT-Grundschutz

4. IT-Grundschutz-Tag 2023 | Nürnberg | 11.10.2023

A hand is shown holding a large, metallic gear. Overlaid on the gear and the hand is a black and white line drawing sketch of several interlocking gears of various sizes. The background is a light blue gradient.

# IT-Grundschutz-Kompendium Edition 2024

Zugunsten „begleitender“ Projekte wenig neue oder überarbeitete Bausteine in 2023  
Parallel: Optimierung interner Prozesse


## -> 2024 soll keine Edition veröffentlicht werden

Weiterhin laufende Veröffentlichung von Community und Final Drafts

Eventuell auftretende Fehler werden in Errata korrigiert

Keine Aufwände bei Anwendern, da nicht auf eine Edition 2024 migriert werden braucht

# Kern-Aktivitäten

- 
- Mapping IT-Grundschutz-Kompendium 2023 zur ISO 27001:2022 sowie (interne) Betrachtung Zusammenspiel zwischen ISO 27001 und IT-Grundschutz
  - Optimierung der Baustein-Struktur
  - Reduzierung der Dokumentationsaufwände im IT-Grundschutz
  - sowie „Weg in die Basis-Absicherung“ und BSI-Standard 200-4



# Zuordnungstabelle ISO/IEC 27001:2022 zum IT-Grundschutz

- Grundlegende Überarbeitung der bestehenden Zuordnungstabelle
- Gegenüberstellung basiert auf:
  - ISO/IEC 27001:2022
  - BSI-Standards 200-1 bis 200-3
  - IT-Grundschutz-Kompendium 2023
- Berücksichtigung neuer Bausteine (z. B. OPS.1.1.1 Allgemeiner IT-Betrieb, NET.3.4 Network Access Control)
- Zuordnungstabelle veröffentlicht

Zuordnungstabelle ISO/IEC 27001:2022 zum IT-Grundschutz

	ISO/IEC 27001:2022	IT-Grundschutz
1	Scope – Anwendungsbereich	BSI-Standard 200-2, Kapitel 1 Einleitung
2	Normative references – Normative Verweisungen	BSI-Standard 200-1, Kapitel 11.1 Literaturverzeichnis
3	Terms and definitions – Begriffe	BSI-Glossar der Cyber-Sicherheit, <a href="https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html">https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html</a>
4	<b>Context of the organization – Kontext der Organisation</b>	
4.1	Understanding the organization and its context – Verstehen der Organisation und ihres Kontextes	<b>BSI-Standard 200-2, Kapitel 3.2.1 Ermittlung von Rahmenbedingungen</b> ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie ORP.5.A1 Identifikation der Rahmenbedingungen
4.2	Understanding the needs and expectations of interested parties – Verstehen der Erfordernisse und Erwartungen interessierter Parteien	<b>BSI-Standard 200-2, Kapitel 3.2 Konzeption und Planung des Sicherheitsprozesses</b> <b>ORP.5.A1 Identifikation der Rahmenbedingungen</b>
4.3	Determining the scope of the information security management system – Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	<b>BSI-Standard 200-2, Kapitel 3.3.4 Festlegung des Geltungsbereichs und Kapitel 8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung</b> ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit
4.4	Information security management system – Informationssicherheitsmanagementsystem	<b>BSI-Standard 200-1, Kapitel 3 ISMS-Definition und Prozessbeschreibung</b> <b>BSI-Standard 200-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz</b> ISMS.1 Sicherheitsmanagement
5	<b>Leadership – Führung</b>	
5.1	Leadership and commitment – Führung und Verpflichtung	<b>BSI-Standard 200-2, Kapitel 3.1 Übernahme von Verantwortung durch die Leitungsebene</b> ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Stand 6. Edition 2023

Optimierung der Baustein-Struktur

## Struktur durch Satzschablonen

Vereinheitlichung der Textstruktur

Fokussierung auf ein prüfbares Ergebnis

Stärkerer Fokus auf das Ziel einer Teilanforderung

Reduktion des Textumfangs

Ein Aspekt pro Teilanforderung



Copyright @ Fotolia

# Aufbau einer Satzschablone (Diskussionsentwurf)

**[{Für, Für alle}] <OBJEKT> <MODALVERB> <ERGEBNIS> <Prozesswort> [<Präzisierung des Ergebnisses>]**

Bestandteile sind ggf. weiter spezifiziert.

Bsp. <Modalverb> := {MUSS, MÜSSEN, SOLLTE [NICHT], SOLLTEN [NICHT]}

- [] Optionaler Bestandteil
- <> Muss durch konkreten Inhalt ersetzt werden
- {} Menge, aus der genau eine Möglichkeit gewählt werden muss

## Beispiel zum Entwurf

### APP.6.A1 bisher:

*„Bevor eine Institution eine (neue) Software einführt, MUSS sie entscheiden, wofür die Software genutzt und welche Informationen damit verarbeitet werden sollen, wie die Benutzenden bei der Anforderungserhebung beteiligt und bei der Einführung unterstützt werden sollen, wie die Software an weitere Anwendungen und IT-Systeme über welche Schnittstellen angebunden wird, [...]“*

### APP.6.A1 neu (Auszug):

- a) Für Software, die beschafft werden soll, MUSS ein Softwarebeschaffungsprozess definiert sein.
- b) Der Softwarebeschaffungsprozess MUSS so gestaltet sein, dass festgelegt wird, für was eine Software, die beschafft werden soll, verwendet wird.
- c) Der Softwarebeschaffungsprozess MUSS so gestaltet sein, dass Benutzende bei der Anforderungserhebung beteiligt werden.

# Was wollen **wir** bei der Dokumentation erreichen?

Dokumen-  
tation  
**vereinfachen**

Dokumentation soll  
**keinem Selbstzweck**  
dienen

Der IT-Grundschutz versteht  
sich als eine Art **Umsetzungsan-  
leitung** zur ISO 27001

**Fokussierung** auf die  
Informationssicherheit

Auflösung des  
Spannungsverhält-  
nis zwischen  
Wünschen nach **klarer**  
**Anleitung/Vorgabe** vs.  
**Freiheit** in der  
Gestaltung

**Für wen?**  
Institutionen  
**beliebiger** Art,  
Branche und  
Größe

**Praxisnah**, handhabbar und  
adaptierbar



# Was meinen wir mit Dokumentationsaufwand?

**Dokumentationsaufwand (DA)**, die *Erhebung und Dokumentation von Informationen*. Dies betrifft vor allem die folgenden Bereiche:

- Dokumentation bei Aufbau, Betrieb, Aufrechterhaltung und kontinuierlicher Verbesserung eines ISMS gemäß BSI-Standards
  - z. B. die Leitlinie für Informationssicherheit oder der IT-Grundschatz-Check
- Dokumentation, die in Anforderungen aus dem IT-Grundschatz-Kompendium gefordert wird oder begleitend notwendig ist
  - z. B. ORP.4 Dokumentation der Benutzerkennungen und Rechteprofile
- Dokumentation, die im Rahmen einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschatz erstellt wird
  - z B. Auditberichte

# Dokumentenpyramide (Entwurf)



## Strategische(r) DA

- Aussagen zu Zielen, Umfeld, Leitgedanken & Rahmenwerken
- Z. B. in: Sicherheitsleitlinie, Cloud-Strategie, Notfall-Strategie

## Taktische DA

- Konkretisierung strategischer DA in (Vorgabe-)Richtlinien für den IV (xy MUSS, SOLLTE, DARF NICHT ...)
- Pro Thema: Geforderte primäre Eigenschaften auf Abstraktionsniveau der Bausteine, der ISO 27001/2

## Operative DA – Gestaltung (Thema)

- individuelle Gestaltung der Themen taktischer DA in Konzepten und Umsetzungsvorgaben
- Bsp.: Kryptokonzept, Notfallkonzept, Passwortvorgaben, ...

## Operative DA – Vermittlung (Adressaten)

- individuelle Vermittlung an die Adressaten der operativen DA
- Bsp.: Arbeitsanweisungen, Checklisten, Schulungsinhalte...

## Operative DA – Ergebnis

- (Notwendige) Ergebnisse gelebter strategischer, taktischer und operativer DA
- Bsp.: Liste Zutrittsbefugter, Netzplan, FW-Konfiguration, Klimaprotokoll Serverraum, ...

## Weitere Ansätze zur Optimierung der Dokumentationsaufwände (Entwurf)

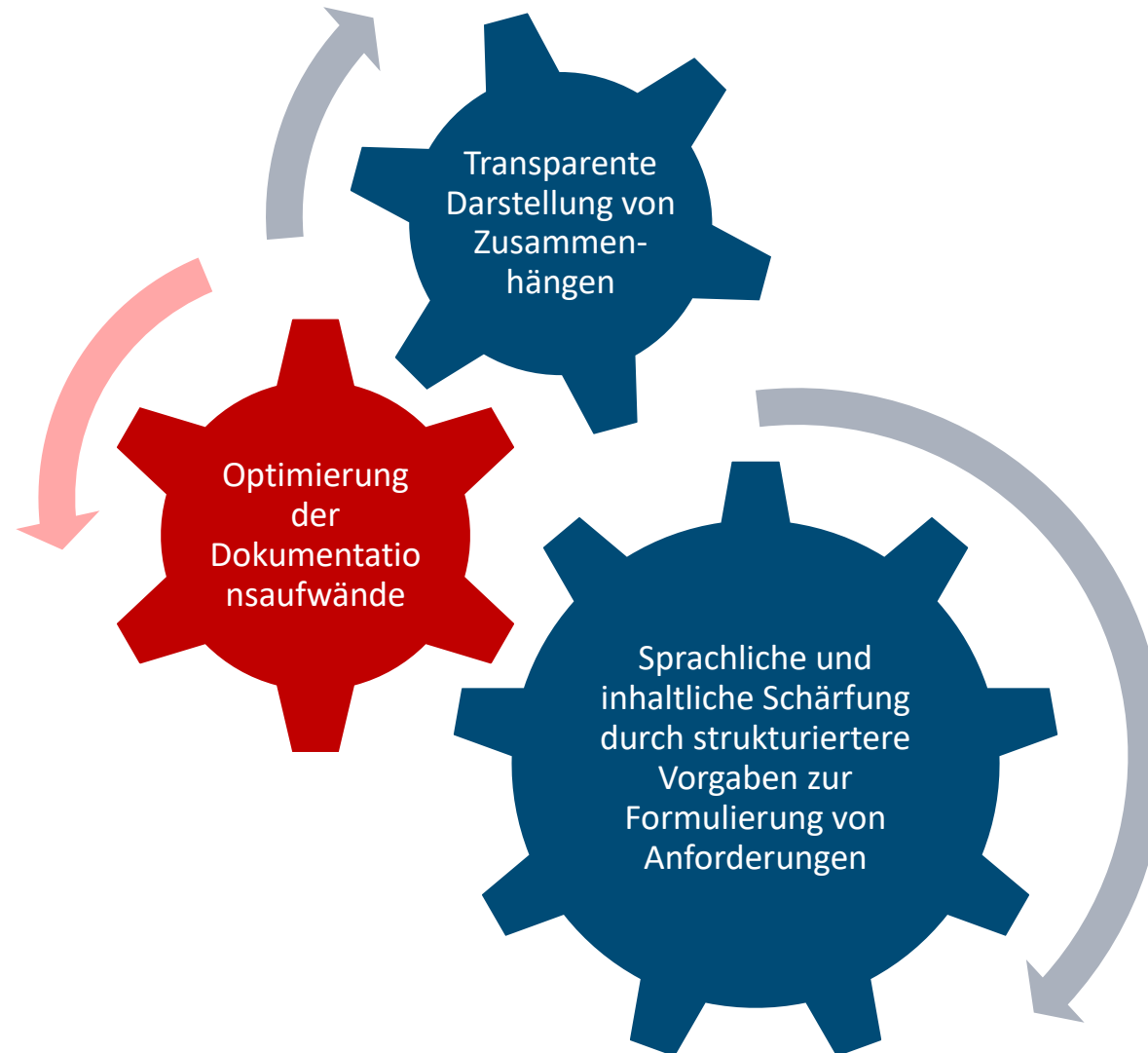
- Gebündelter Einstieg zu ITGS-DAs im BSI-Standard 200-2 und Kompendium
  - Erläuterungen und Übersicht über alle DAs
- Hinweise zu den Formaten der DA und Freiheiten in der Gestaltung der DA
  - Je nach DA-Kategorie (Dokumentenpyramide) angepasste Anforderungen an das Format, Lenkung, Möglichkeit zur Automatisierung
- Vermeidung redundanter Nennung und Forderung von DAs
  - Zentrale Übersicht je DA über die Quellen/Referenzierungen
- Jeder Baustein informiert über seine notwendigen DAs
  - Klärung, welche DAs für welche Anforderungen eines Bausteins erstellt werden müssen
  - Bezug zu bausteinübergreifenden DAs transparent darstellen
- Konsolidierung und Zusammenführung von DAs

## Weitere Ansätze zur Optimierung der Dokumentationsaufwände (Entwurf)

- IT-Grundschutz-Tool-freundliche Umsetzung der Baustein-DA-Anteile geplant
  - Vorherige Vorschläge sollten idealerweise in Tools abgebildet werden (können) und Automatisierungen ermöglichen.
- Einheitlichere Nennung und Vermittlung der DAs in den Quellen
  - Wording, Bezug, Darstellung von Zusammenhängen, Aufteilung der Themen
- Einführung eines Gremiums engagierter IT-Grundschutz-Anwender zur Erzeugung praxisnaher DA-Inhalte und Vorlagen
  - Generelles Interesse zur Teilnahme in dieser Runde?



# Ganzheitliche Weiterentwicklung des IT-Grundschutzes



Erweiterung Personenzertifizierung

## BCM-Praktiker

Unabhängige Ergänzung zum IT-Grundschutz-Berater und -Praktiker

Umfang: 24 Zeitstunden

Schulung und Prüfung durch Schulungsanbieter

Fokus auf BC-Bs und BC-Interessierte

Abstimmungen laufen



Copyright @ Fotolia

# IT-Grundschutz-Tage 2024

- 2024 keine IT-Grundschutz-Tage
- Evaluierung und Neukonzeption des bisherigen Konzepts
- Ziel: Den Erfahrungsaustausch mit den Anwendenden weiterhin zielgruppenspezifisch, praxisorientiert und informativ zu gestalten.



Copyright @ Fotolia



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
Digital•Sicher•BSI

# Vielen Dank für Ihre Aufmerksamkeit!

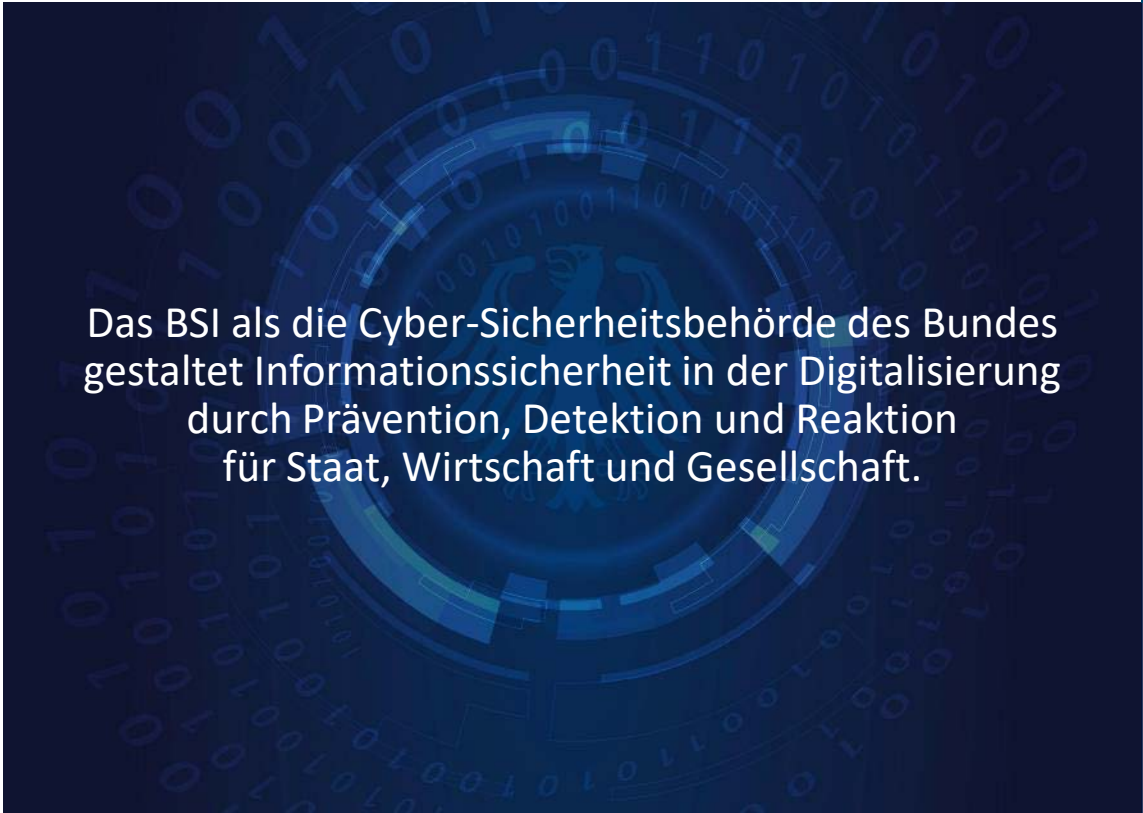
Deutschland  
**Digital•Sicher•BSI**

## Holger Schildt

Referatsleiter „BSI-Standards und IT-Grundschutz“

[it-grundschutz@bsi.bund.de](mailto:it-grundschutz@bsi.bund.de)

Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Godesberger Allee 185-189  
53175 Bonn  
[www.bsi.bund.de](http://www.bsi.bund.de)



Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.