Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

3. IT-Grundschutz-Tag 2023

Organisatorische Resilienz mit IT-Grundschutz:

Von der Informationssicherheit zur Business Continuity

Aktuelles und Diskussion zum IT-Grundschutz

Holger Schildt, Referatsleiter BSI-Standards und IT-Grundschutz

3. IT-Grundschutz-Tag 2023 | Limburg | 14.06.2023

Veröffentlichungsprozess

Arbeitsentwürfe
(Working Drafts)

- sehr grobe Entwürfe
- nur BSI-interne Verwendung

Community-Entwürfe
(Community Drafts)

- akzeptabler Reifegrad
- Grundlage für die Diskussion mit der Community

Finaler Entwurf
(Final Draft)

- nach Einbindung der relevanten Kommentare der Community

Edition

- aktuell gültige IT-Grundschutz-Fassung
- Veröffentlichung Print (kostenpflichtig) und Digital (kostenlos) im Februar

Änderungen Edition 2023

10 Bausteine neu erstellt

21 Bausteine inhaltlich überarbeitet

3 Bausteine entfallen

- SYS.2.2.2 Clients unter Windows 8.1
- OPS.2.1 Outsourcing für Kunden und OPS.3.1 Outsourcing für Dienstleister

Überarbeitung Kreuzreferenztabellen zu elementaren Gefährdungen

Geschlechtergerechtere Sprache, führte zur Umbenennung von 14 Rollen, z.B.

- Generell: Verwendung Plural (*beauftrage statt *beauftragter)
- Benutzer -> Benutzende, Mitarbeiter -> Mitarbeitende etc.

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)
- Veröffentlichung der Zuordnungstabelle Ende Juli 2023 geplant

Zuordnungstabelle ISO/IEC 27001:2022 zum IT-Grundschutz

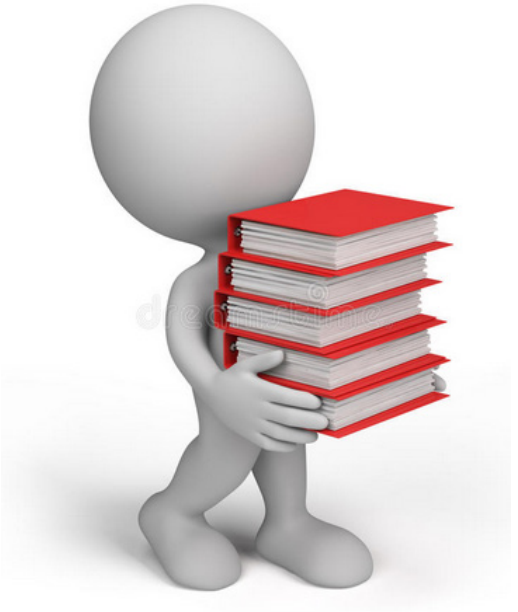
		ISO/IEC 27001:2022	IT-Grundschutz
1		Scope – Anwendungsbereich	BSI-Standard 200-2, Kapitel 1 Einleitung
2		Normative references – Normative Verweisungen	BSI-Standard 200-1, Kapitel 11.1 Literaturverzeichnis
3		Terms and definitions – Begriffe	BSI-Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html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

Bundesamt für Sicherheit in der Informationstechnik (BSI) Stand 6. Edition 2023

Reduzierung der Dokumentationsaufwände im IT-Grundschutz

Mit externem Projekt werden die drei folgenden, aufeinander aufbauenden Projektziele verfolgt:

1. Erstellung eines umfassenden **Überblicks** über die im IT-Grundschutz geforderten Dokumentationsaufwände
2. **Analyse** und **Bewertung** der im IT-Grundschutz geforderten Dokumentationsaufwände
3. Erarbeitung von **Empfehlungen zur Optimierung** der im IT-Grundschutz geforderten Dokumentationsaufwände



©dreamstime

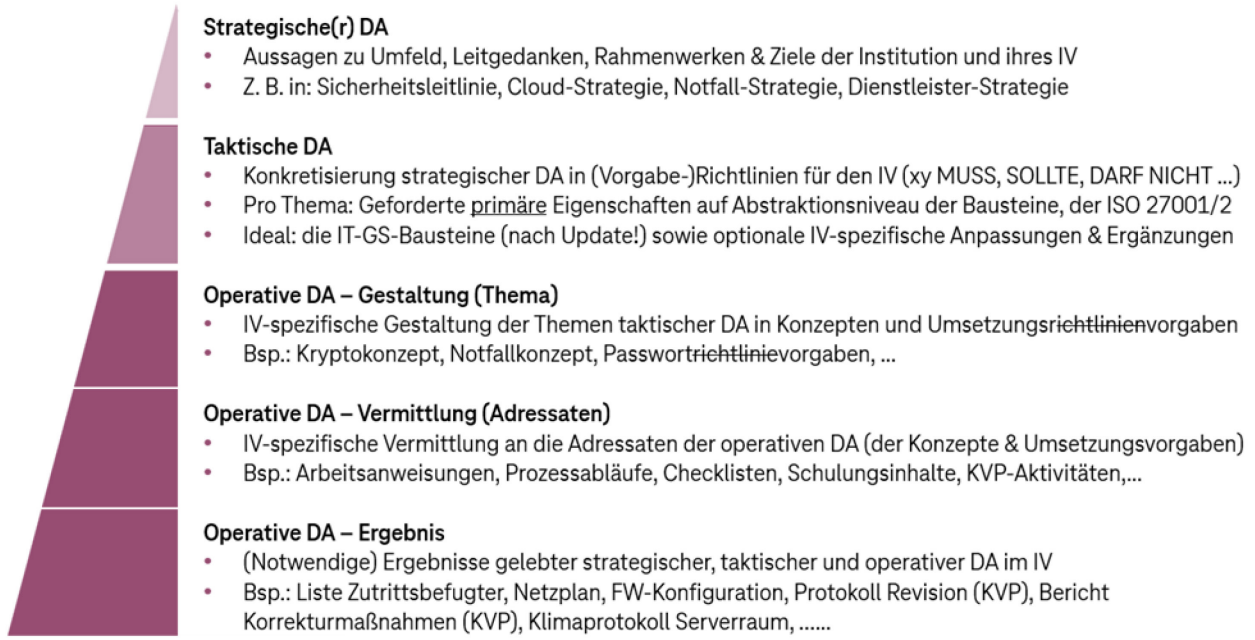
Projektstatus:
Erster Meilenstein zur Erfassung der IST-Situation erfolgreich abgeschlossen

Zwischenergebnisse

Erarbeitung einer **transparenteren** Dokumentenhierarchie auf Basis der Analyse der IST-Situation:

Mit dem **Ziel** der Vereinfachung durch

- Klarerer, transparenterer, wiederkehrender Struktur
- Vereinfachung durch Auflösung von Redundanzen
- Fokussierung auf Themen der Informationssicherheit



Die hier vorgestellten Themen und Lösungsansätze spiegeln den aktuellen Arbeitsstand wieder und sind nicht final. Es wird gerade ein Proof of Concept anhand beispielhafter Bausteine zur Verifikation dieses Ansatzes erstellt.

IT-Grundschutz-Berater und IT-Grundschutz-Praktiker

- Fast 150 IT-Grundschutz-Berater
- Das Schulungskonzept des BSI stellt ein einheitliches hohes Niveau an fachlicher Expertise sicher.
- Es besteht eine große Auswahl an Dienstleistern, doch wer hat die von mir benötigte Expertise?
- Für einen Informationssicherheitsprozess fehlt es in vielen Institutionen an der entsprechenden Expertise.
- Aus der kontinuierlich hohen Bedrohungslage und der schnell voranschreitenden Digitalisierung erwächst mehr und mehr der Bedarf an Informationssicherheit.
- ca. 55 Schulungsanbieter

- **Ausbildung von fast 4500 IT-Grundschutz-Praktikern seit 2019**

Erweiterung Personenzertifizierung

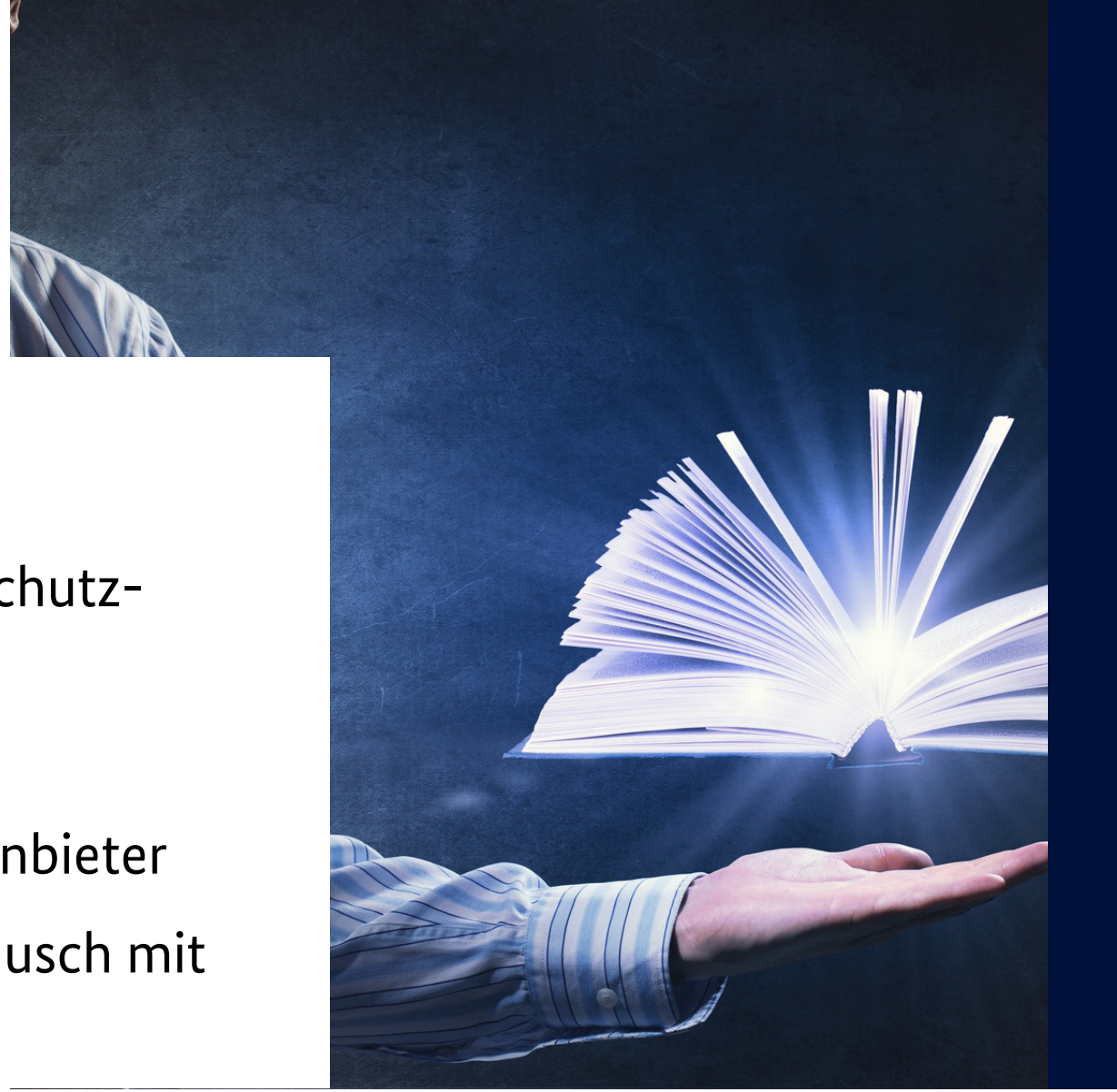
BCM-Praktiker (in Diskussion)

Unabhängige Ergänzung zum IT-Grundschutz-Berater und –Praktiker

Umfang: 24 Zeitstunden

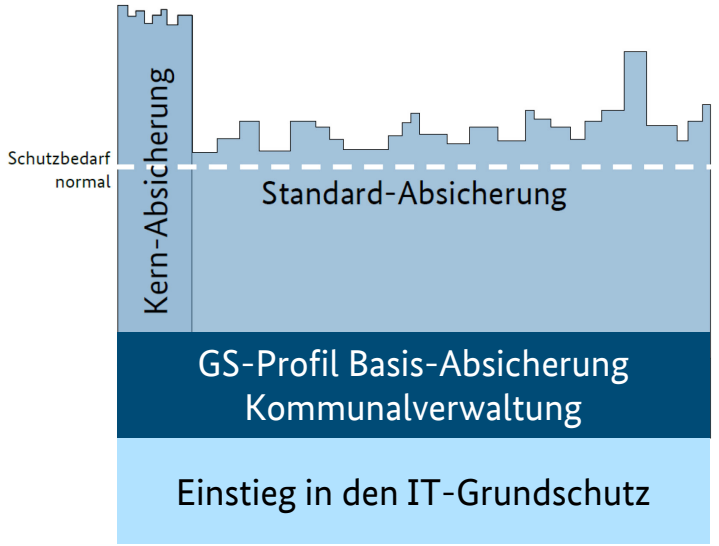
Schulung und Prüfung durch Schulungsanbieter

Diskussion auf nächsten Erfahrungsaustausch mit Schulungsanbietern



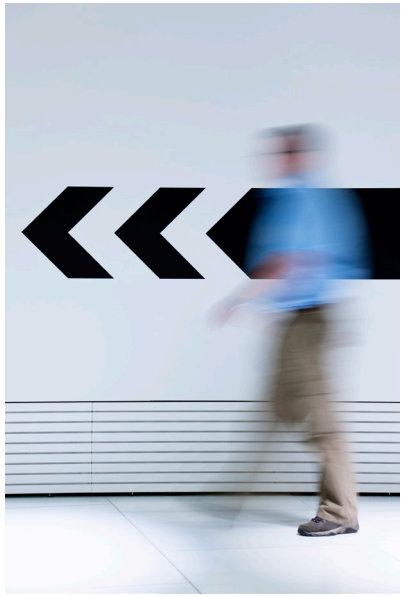
Ausgangslage und Lösungsansatz

- Einstieg in den IT-Grundschutz trotz Basis-Absicherung teilweise zu komplex: vielen kleinen Institutionen fehlen ausreichend Ressourcen und Know-how
- Im Fokus des „Weges in die Basis-Absicherung“: Kommunen
- Ziel: Ohne (tiefere) Kenntnis der Methodik können Sachstände erhoben und umzusetzende Anforderungen mittels Prüffragen und Checklisten mit wenig Aufwänden identifiziert werden.
- Es werden Hilfsmittel bereitgestellt, die bei der Umsetzung unterstützen
- Im Anschluss kann das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ nahtlos umgesetzt werden.



Vorgehensweise

- Clusterung der **51** relevanten Bausteine in **18** themenspezifischen Checklisten
  - Festlegung eines möglichst praxisnahen Sicherheitsniveaus für den Einstieg (Reduktion auf wesentliche Anforderungen/Maßnahmen)
  - Bereitstellung von Hilfsmitteln / weitergehenden Informationen zur Unterstützung
  - Formulierung von konkreten Fragen
  - Verschmelzung von verschiedenen Bausteinanforderungen zu (thematisch sortierten) Prüffragen
  - Kostenschätzung (Kategorie 1 bis 4) zur Erleichterung der Priorisierung der Maßnahmen
- Einbindung von Modellkommunen: über kommunale Spitzenverbände



IT-Grundschutz-Kompendium Edition 2024

Zugunsten „begleitender“ Projekte nur wenig neue oder überarbeite Bausteine in 2023

Parallel: Optimierung interner Prozesse

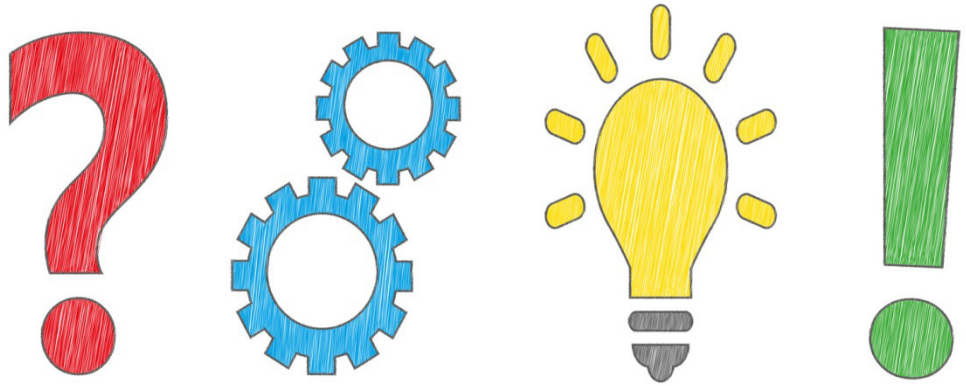
-> 2024 soll keine Edition veröffentlicht werden

Weiterhin laufende Veröffentlichung von Community und Final Drafts

Eventuell auftretende Fehler werden in Errata korrigiert

Keine Aufwände bei Anwendern, auf Edition 2024 zu migrieren

Gerne jetzt oder später



Geplante IT-Grundschutz-Tage 2023

- *1. IT-Grundschutz-Tag: 2. März 2023*
- 2. IT-Grundschutz-Tag: 25. April 2023
- 3. IT-Grundschutz-Tag: 14. Juni 2023
- 4. IT-Grundschutz-Tag: 11. Oktober 2023

Bleiben Sie im Kontakt

- IT-Grundschutz-Hotline:
  it-grundschutz@bsi.bund.de
  (0)22899-9582-5369
- Twitter: @BSI_Bund, #ITGrundschutz

Vielen Dank für Ihre Aufmerksamkeit!

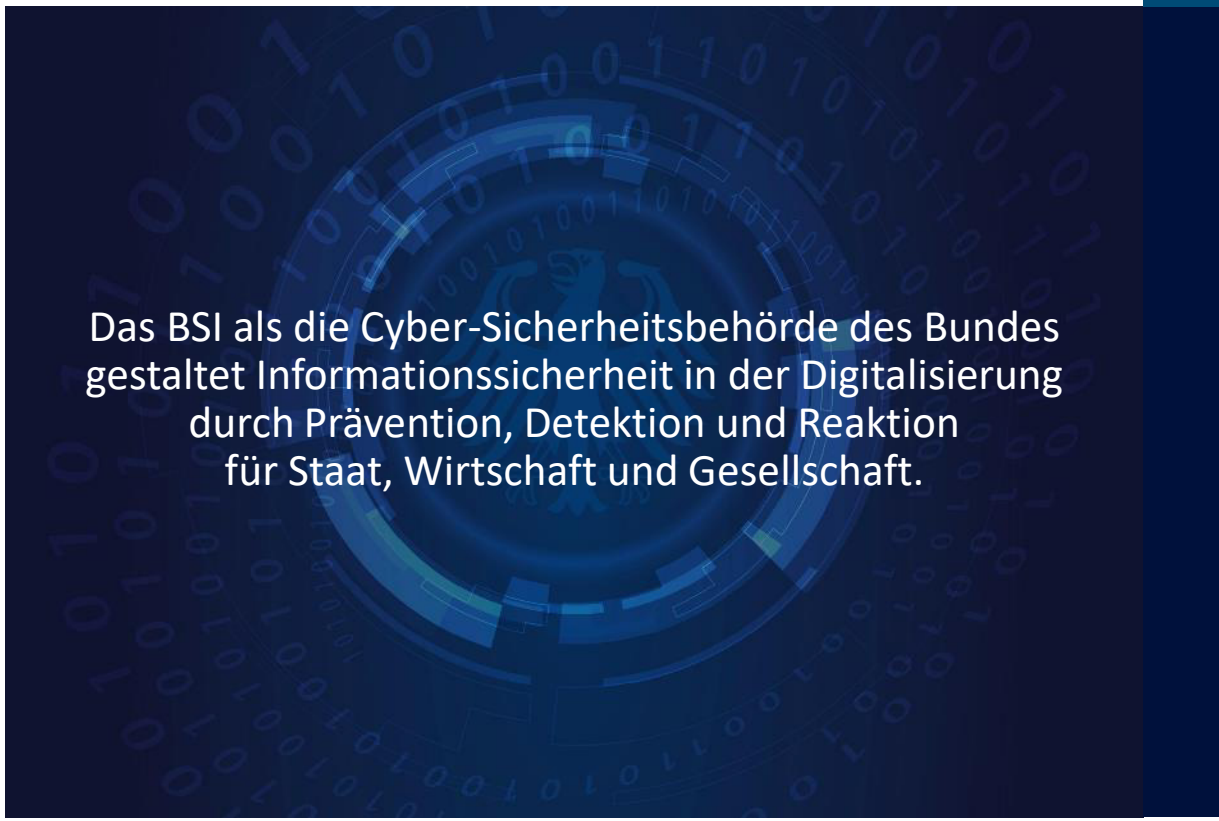
Deutschland
Digital•Sicher•BSI•

Holger Schildt

Referatsleiter „BSI-Standards und IT-Grundschutz“

it-grundschutz@bsi.bund.de

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



Bundesamt
für Sicherheit in der
Informationstechnik