Fortentwicklung des IT-Grundschutzes zu IT-Grundschutz++

Vom Brockhaus zum Wiki

Bundesamt
für Sicherheit in der
Informationstechnik

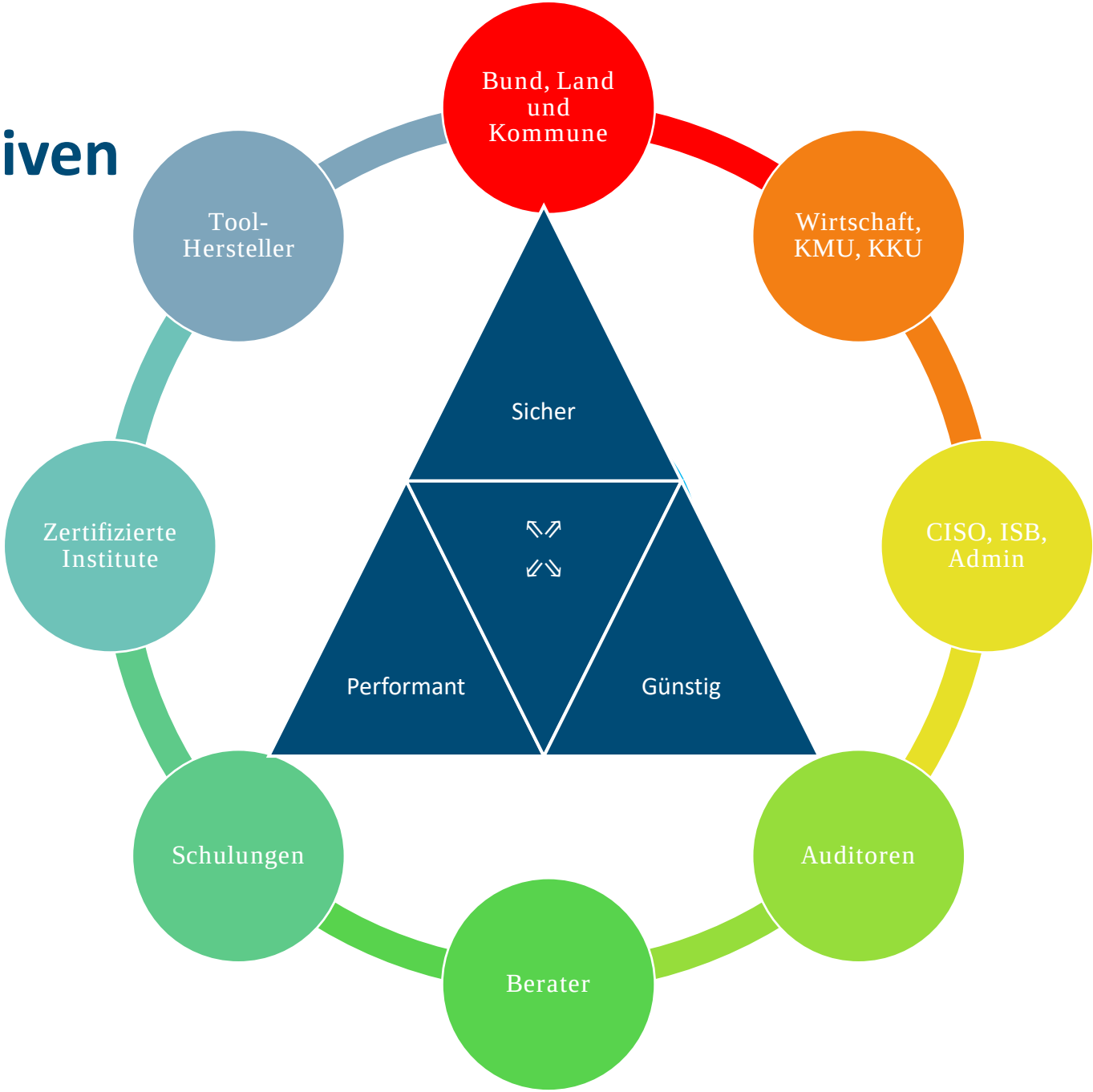
Holger Schildt, Referatsleiter S 13 - IT-Grundschutz

verinice.XP 2024 | Berlin | 19.02.2025

01. Motivation

Stakeholder und Perspektiven

Viele Brillen, ein Bild



Vision IT-Grundschutz++

Wer Visionen hat, soll zum BSI gehen

Cybersicherheit ist mess- & automatisierbar:

Sicherheitsanforderungen werden als priorisierte, maschinenlesbare Regeln in kontinuierlichen PDCA-Zyklen erstellt

Automatisierung des ISMS

Anwendung datengesteuerter Werkzeuge weitgehend ermöglichen

Erfassung

- Systeme
- Daten
- Lieferanten

Integration

- Continuous Integration, Delivery and Deployment
- Smart Standards
- Smart Contracts

Aufrechterhaltung

- Überwachung der Konformität
- Sperrung
- Alarmierung

Redundant arbeiten soll die Technik, nicht der Mensch

Integration der Perspektiven

SYS.3.1.A12 Verlustmeldung für Laptops [Benutzer] (S)

Benutzer SOLLTEN umgehend melden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in der Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Die darauf eingesetzte Software inklusive des Betriebssystems SOLLTE komplett neu installiert werden.

SYS.3.1.A13 Verschlüsselung von Laptops (S)

In Laptops verbaute Datenträger wie Festplatten oder SSDs SOLLTEN verschlüsselt werden.

SYS.3.1.A14 Geeignete Aufbewahrung von Laptops [Benutzer] (S)

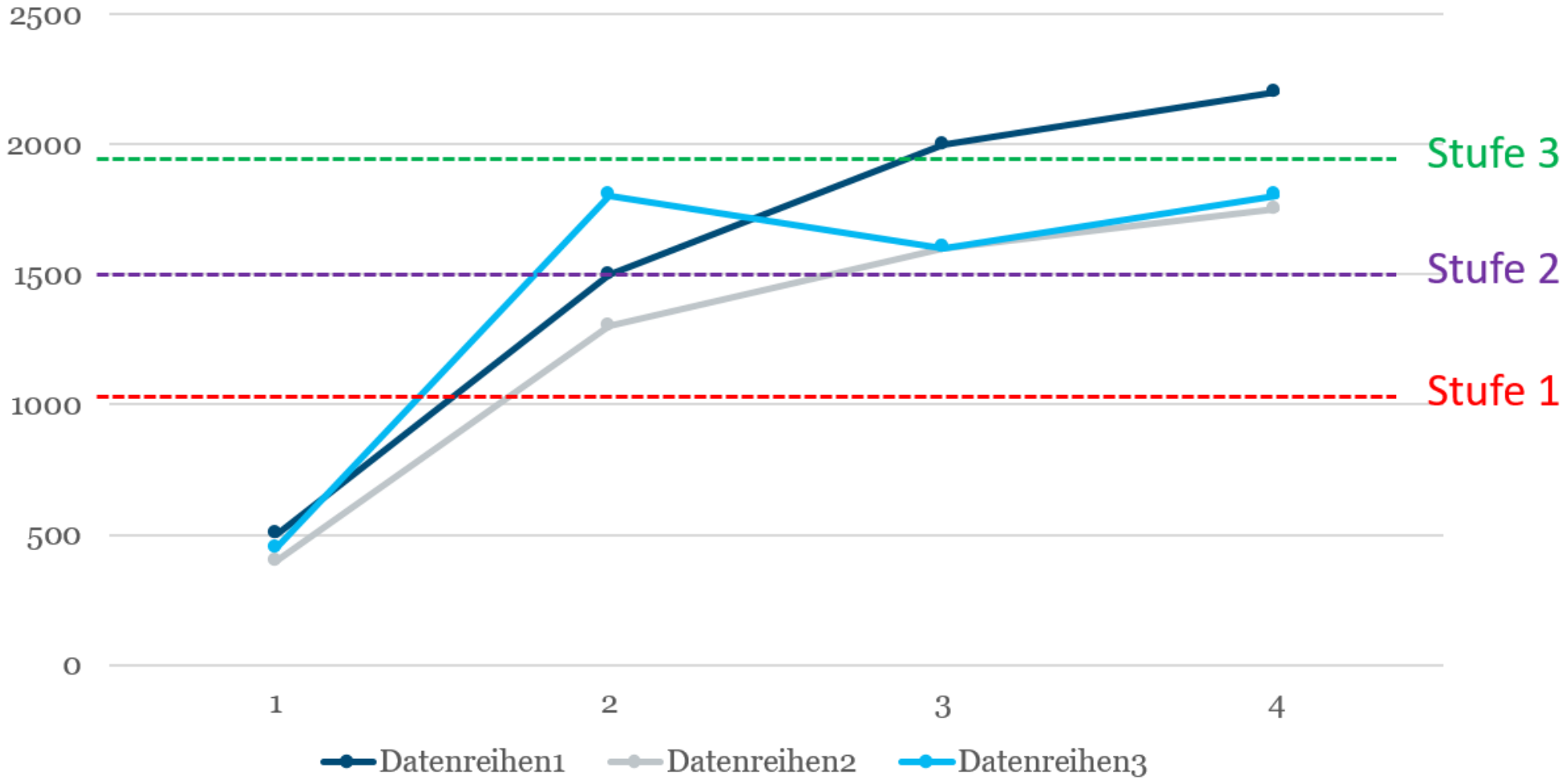
Alle Benutzer SOLLTEN darauf hingewiesen werden, wie Laptops außerhalb der Institution sicher aufzubewahren sind. Abhängig vom Schutzbedarf der darauf gespeicherten Daten SOLLTEN Laptops auch in den Räumen der Institution außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt werden.

SYS.3.1.A15 Geeignete Auswahl von Laptops [Beschaffungsstelle] (S)

Bevor Laptops beschafft werden, SOLLTEN die Zuständigen eine Anforderungsanalyse durchführen. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden. Die Beschaffungsentscheidung SOLLTE mit dem IT-Betrieb abgestimmt sein.

Kennzahlen für Entscheider

Resilienz wird messbar, vergleichbar und verständlich durch Kennzahlindikatoren



02. Neue Möglichkeiten

Vom Baustein zur Praktik

Praktiken als Prozesse des ISMS

Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

Praktiken

- Prozesse des ISMS
- Strategie, Taktik, Operativ

Handlungsworte

- Definierte Tätigkeiten
- Mensch oder Maschine

Zielobjekte

- Technik: Server, Linux, …
- Organisatorisch:
  Standorte, Adressaten, Verträge, …

Hinweise

- Ziele und Definitionen
- Umsetzungshinweise

Stufe 1-5

- Von Quick-Win bis Nice-to-have
- Von Jeder bis erhöhter Schutzbedarf

Tags

- Querschnittsthemen
- Trends im Fokus

03. …und wie?

Bild: © AdobeStock/Azazul

Ebenen der Abstraktion

Flughöhen im Zusammenhang

Geschäfts- und Sicherheitsziele

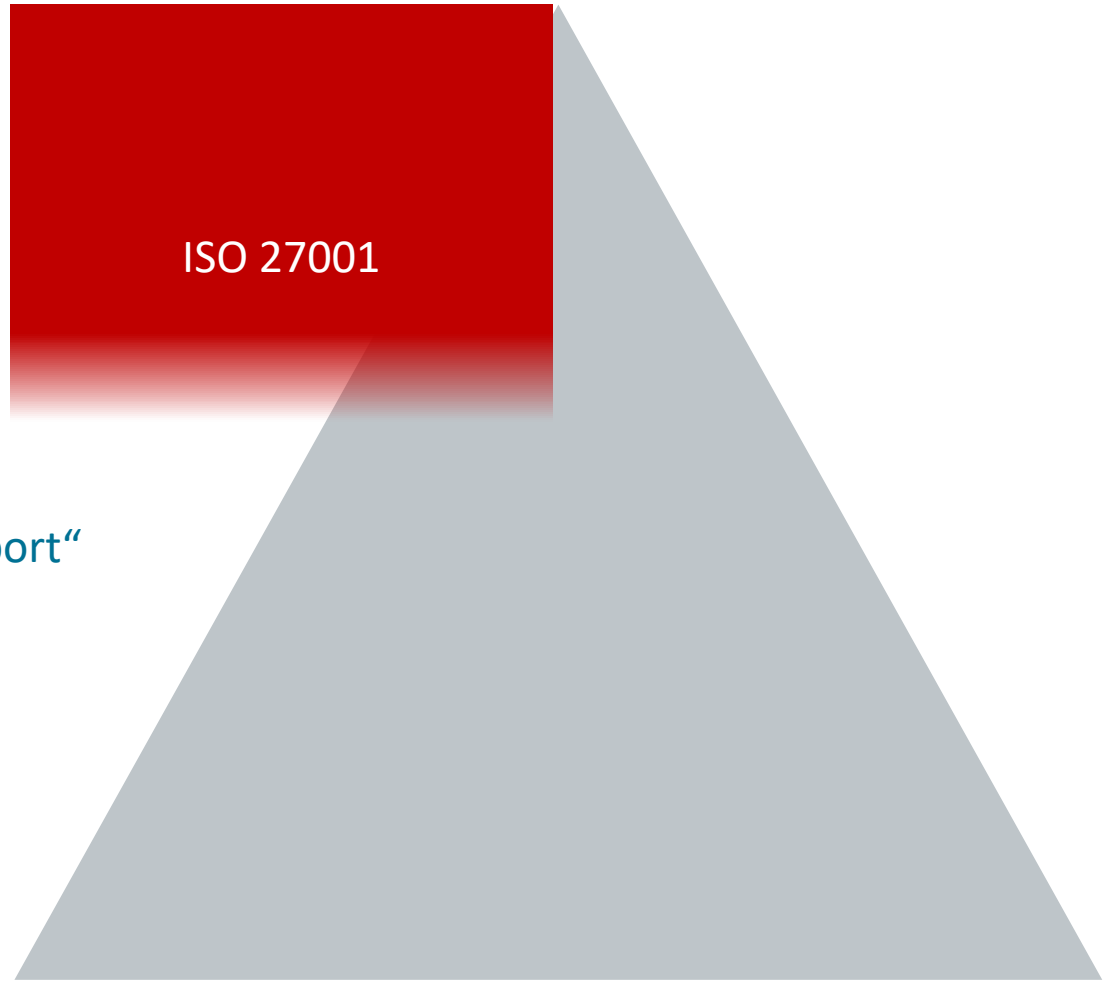
„Vertraulichkeit für unsere Daten“

Lösungsneutrale Prinzipien

„Anwendungen verschlüsseln Daten beim Transport“

Lösungsspezifikation

„Verschlüsselung mit AES256 im CBC-Modus “



Ebenen der Abstraktion

Flughöhen im Zusammenhang

Geschäfts- und Sicherheitsziele

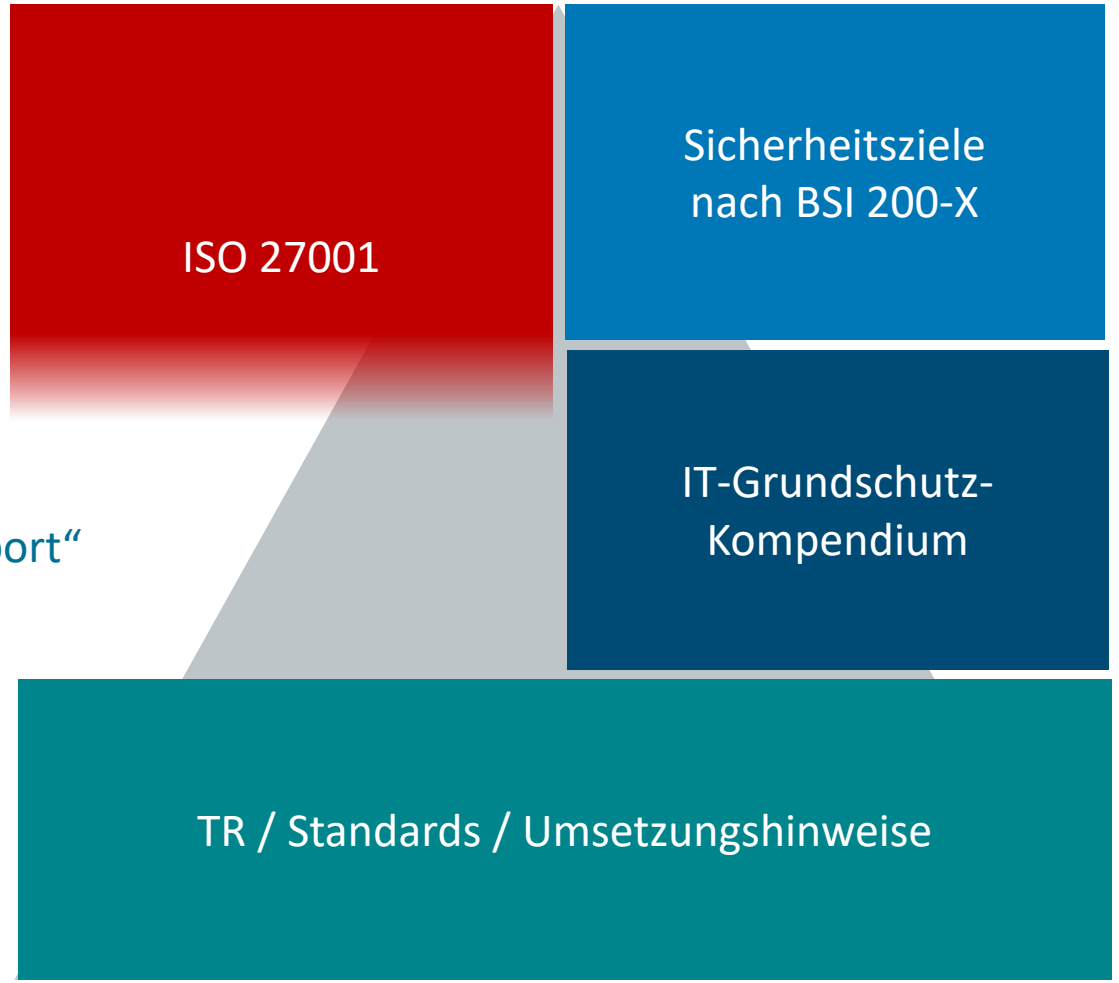
„Vertraulichkeit für unsere Daten“

Lösungsneutrale Prinzipien

„Anwendungen verschlüsseln Daten beim Transport“

Lösungsspezifikation

„Verschlüsselung mit AES256 im CBC-Modus “



Struktur für Anforderungen durch Satzschablonen

Von Johann zu JSON

{Praktik} [für {Zielobjekt}] {MODALVERB} <Ergebnis> {Handlungswort}

Beispiele:

- Die Praktik „Konfiguration“ für IT-Systeme SOLLTE die Änderung von Default-Passwörtern vor der ersten Verwendung festlegen.
- Die Praktik „IT-Betrieb“ SOLLTE die Installation von Software-Aktualisierungen (Updates oder Patches) auf das vom Hersteller bereitgestellte Patchlevel überprüfen.
- Die Praktik „Sensibilisierung“ für Benutzende SOLLTE die Weitergabe von personengebundenen Authentisierungsmitteln verbieten.

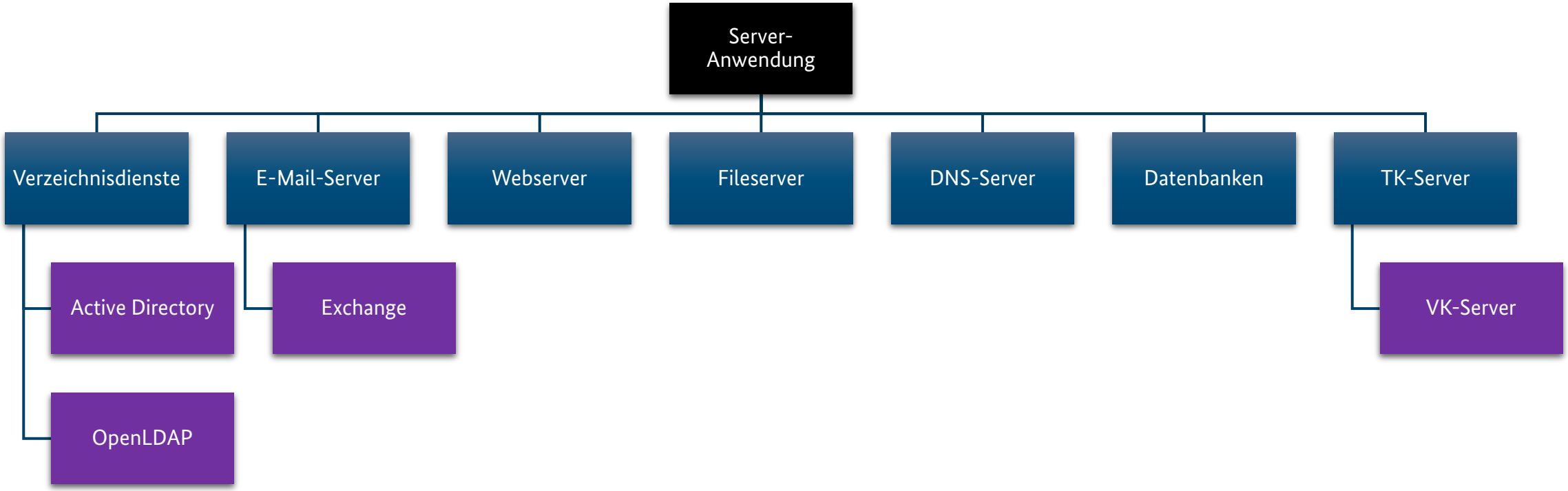
Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

Praktik	Zielobjekt	MODALVERB	Ergebnis	Handlungswort	Hinweis	Tags
Konfiguration	IT-Systeme	SOLLTE	nicht benötigte Funktionen	deaktivieren	Deinstallieren oder Deaktivieren Sie Funktionen, die für Betrieb oder Sicherheit nicht benötigt werden, z.B. ungenutzte Cloud-Anbindungen, Module oder Einstellungen.	Hardening
Sensibilisierung	Benutzende	SOLLTE	die Weitergabe von personengebundenen Authentisierungsmitteln	verbieten	Personengebundene Authentisierungsmittel sind z.B. Passworte, Private PKI-Schlüssel oder Mehr-Faktor-Authentifizierungstoken wie Smartcards.	
Detektion	VPN-Gateways	SOLLTE	VPN-Verbindungen auf unberechtigte Einwahlen	überprüfen	Kann manuell oder durch automatische Analyse von Logdateien erfolgen. Dabei kann z.B. nach ungewöhnlichen vielen fehlgeschlagenen Anmeldungen, veralteten Berechtigungen, Einwahlen von Adminaccounts, ungewöhnlichen Einwahlorten/IP-Adressbereichen/User Agents oder Uhrzeiten gesucht werden.	Zero Trust, Advanced Persistent Threats (APT)

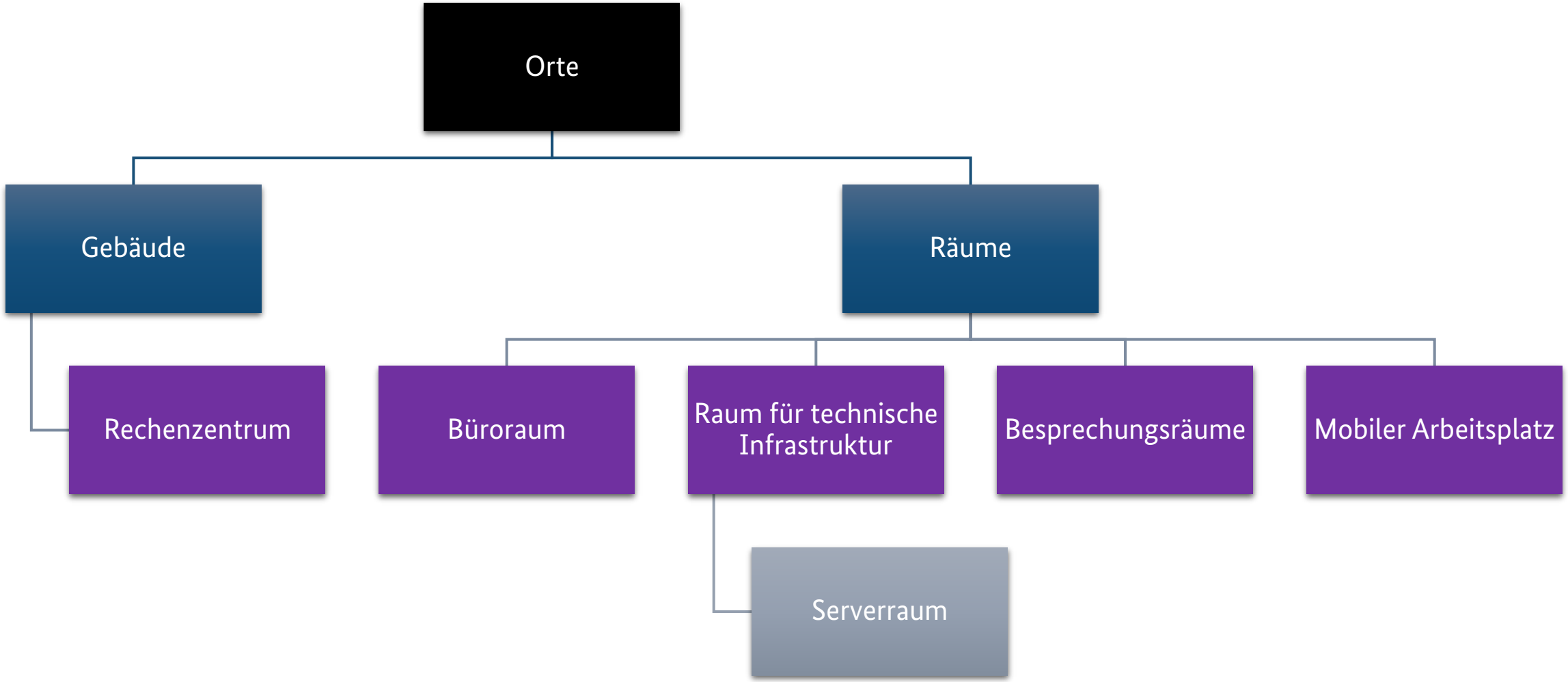
Filter: Technische Zielobjekte

Anforderungen horizontal und vertikal abhaken



Filter: Organisatorische Zielobjekte

Anforderungen werden Adressaten- und Standortgerecht



Filter: Handlungsworte

Zeit sparen, Klarheit gewinnen

- o aktivieren
- o anweisen
- o dokumentieren
- o fordern
- o sensibilisieren
- o installieren
- o protokollieren
- o testen
- ✓ überprüfen

Definition „ÜBERPRÜFEN“

Hierunter versteht man das systematische und vollständige Untersuchen eines Gegenstands (z. B. einer Anlage, Maschine oder eines Verfahrens) mit dem Ziel, die Einhaltung der Anforderung (Konformität) eindeutig festzustellen oder im Falle von Abweichungen wiederherzustellen.

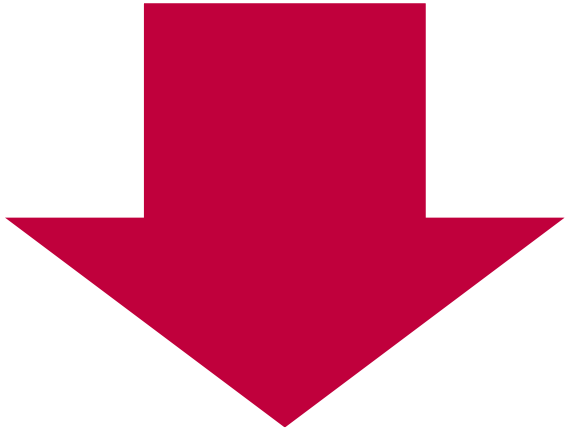
Sichergestellt sein muss dabei insbesondere, dass die Regelmäßigkeit der Überprüfung gewährleistet wird, z.B. durch einen Kalendereintrag oder ein automatisiertes System zur Überprüfung und Alarmierung. Eine Überprüfung gilt erst dann als abgeschlossen, wenn die Konformität positiv bestätigt oder erneut hergestellt wurde; sollte die Wiederherstellung der Konformität nicht durch andere Maßnahmen möglich sein, muss der betrachtete Gegenstand außer Betrieb genommen werden, bis die erforderliche Konformität gewährleistet ist.

Fachinhalte im Fokus

Reduktion der Masse, nicht der Sicherheit

Fokussiert

- Konkretisierung: Was ist wann zu erreichen
- Hinweise: Zweck, Definitionen, Umsetzung
- Neuerungen: NIS2, Videokonferenz-Server



Reduziert

- Anforderungen ohne klares Sicherheitsziel
- Doppelungen

Wo bleibt das (Sicherheits-)Niveau?

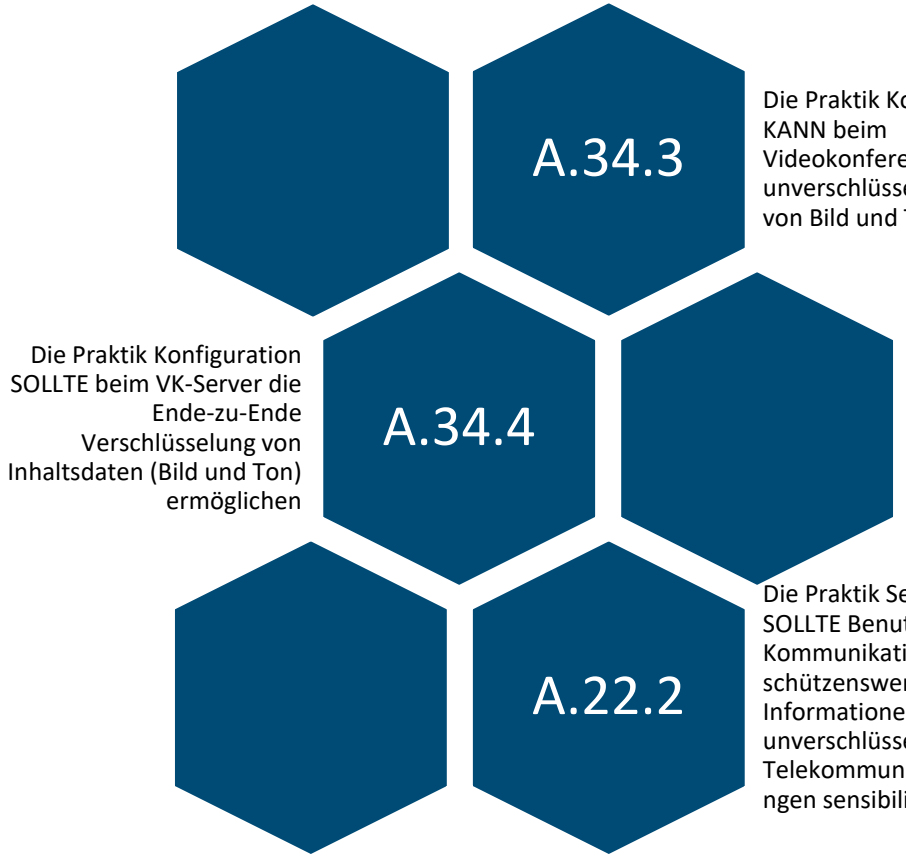
Zukünftige Mess- und Vergleichbarkeit im IT-Grundschutz

IT-Grundschutz

Basis-Anforderungen
- Mindestniveau

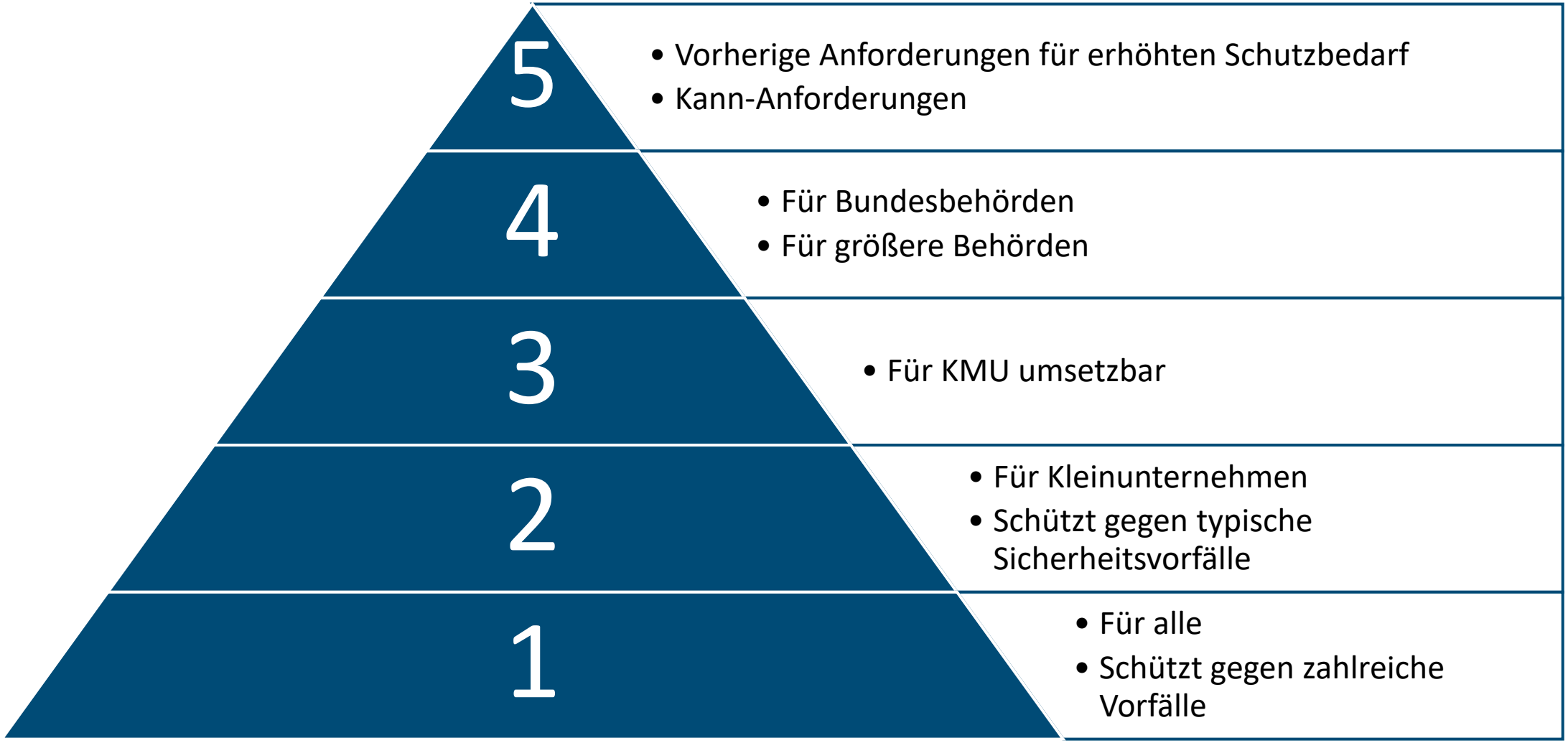
Standard-Anforderungen
- Erweiterung des Niveaus

Anforderungen für einen erhöhten Schutzbedarf
- Risikobasierte Erweiterung



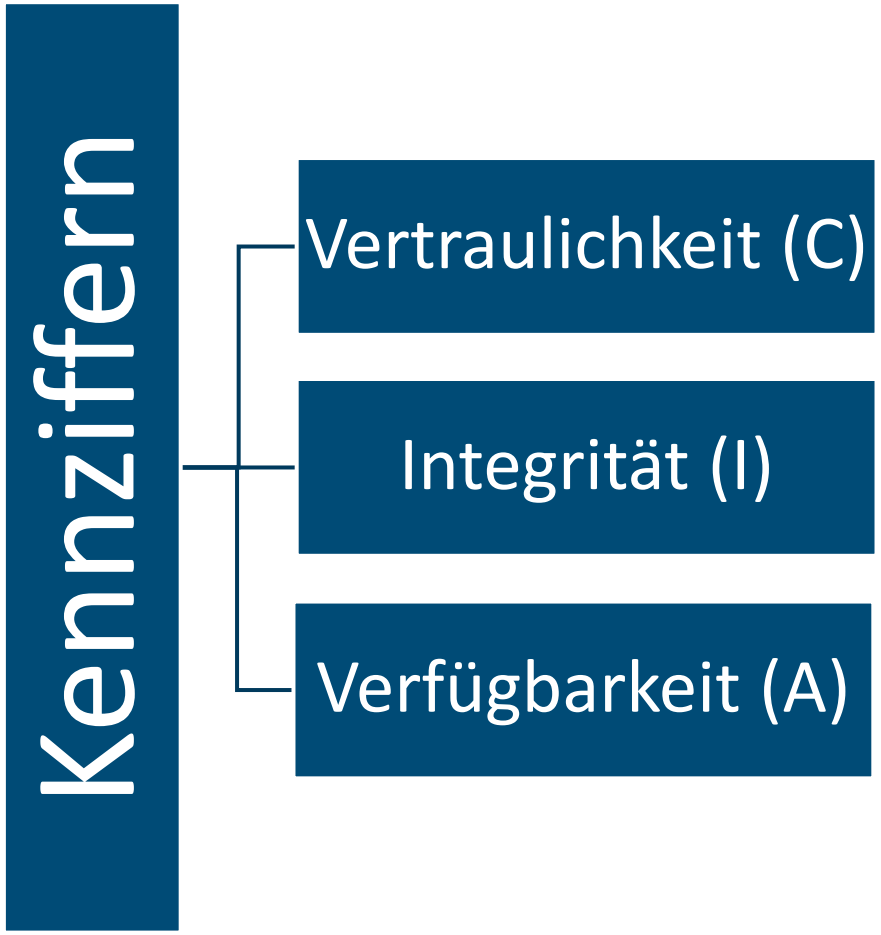
Die Stufen

Was mache ich zuerst



Die Leistungskennzahlen

Was bringt mir eine Anforderung?



Wie Effektiv ist die Anforderung in der Behandlung EINER Gefährdung

Die Schwellwerte

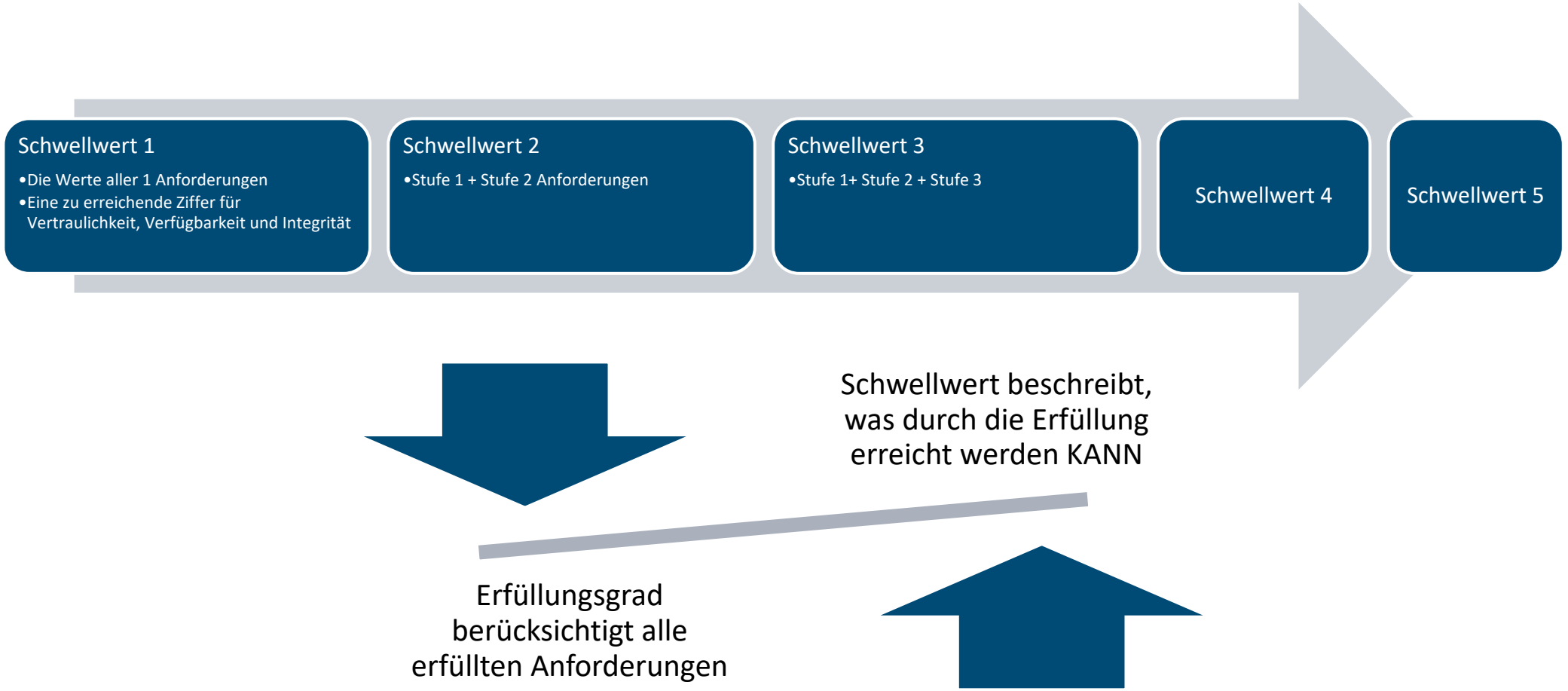
[Stufe 1] Sensibilisierung gegen die Bild- und Tonaufzeichnung ohne vorherige Ankündigung an alle Betroffenen	• Vertraulichkeit : 6 • Integrität: 0 • Vertraulichkeit 0
[Stufe 1] Der IT-Betrieb legt zeitnahe Installation von Sicherheitsupdates fest	• Vertraulichkeit [4] • Integrität [3] • Verfügbarkeit [4]
[Stufe 1] ….	• Vertraulichkeit [X] • Integrität [Y] • Verfügbarkeit [Z]

Schwellwert 1

- ☐ Vertraulichkeit [10+X]
- ☐ Integrität [3+Y]
- ☐ Verfügbarkeit[4+Z]

Die Schwellwerte

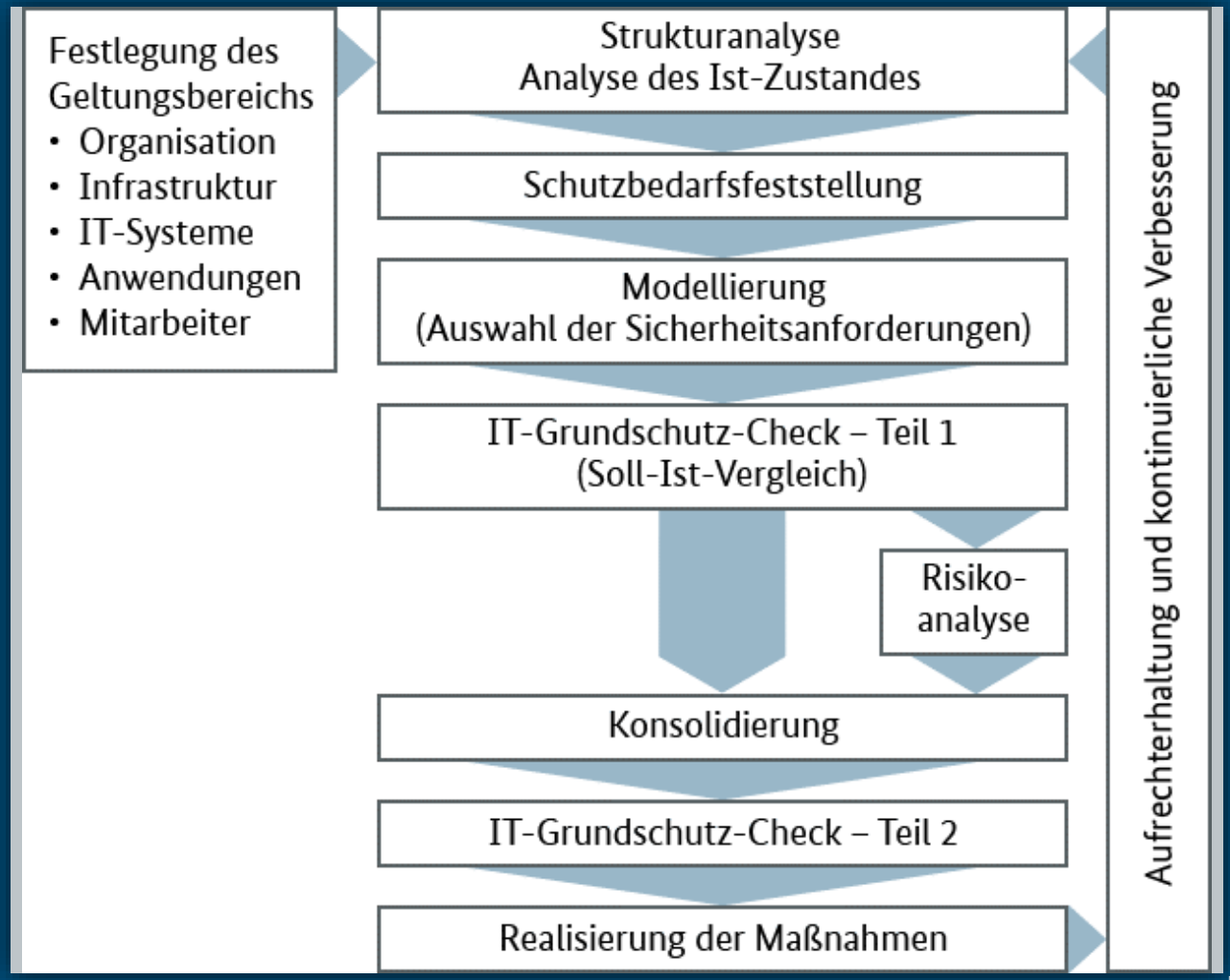
Zusammenspiel mit Erfüllungsgrad



Quick-Start-Guide IT-Grundschutz++

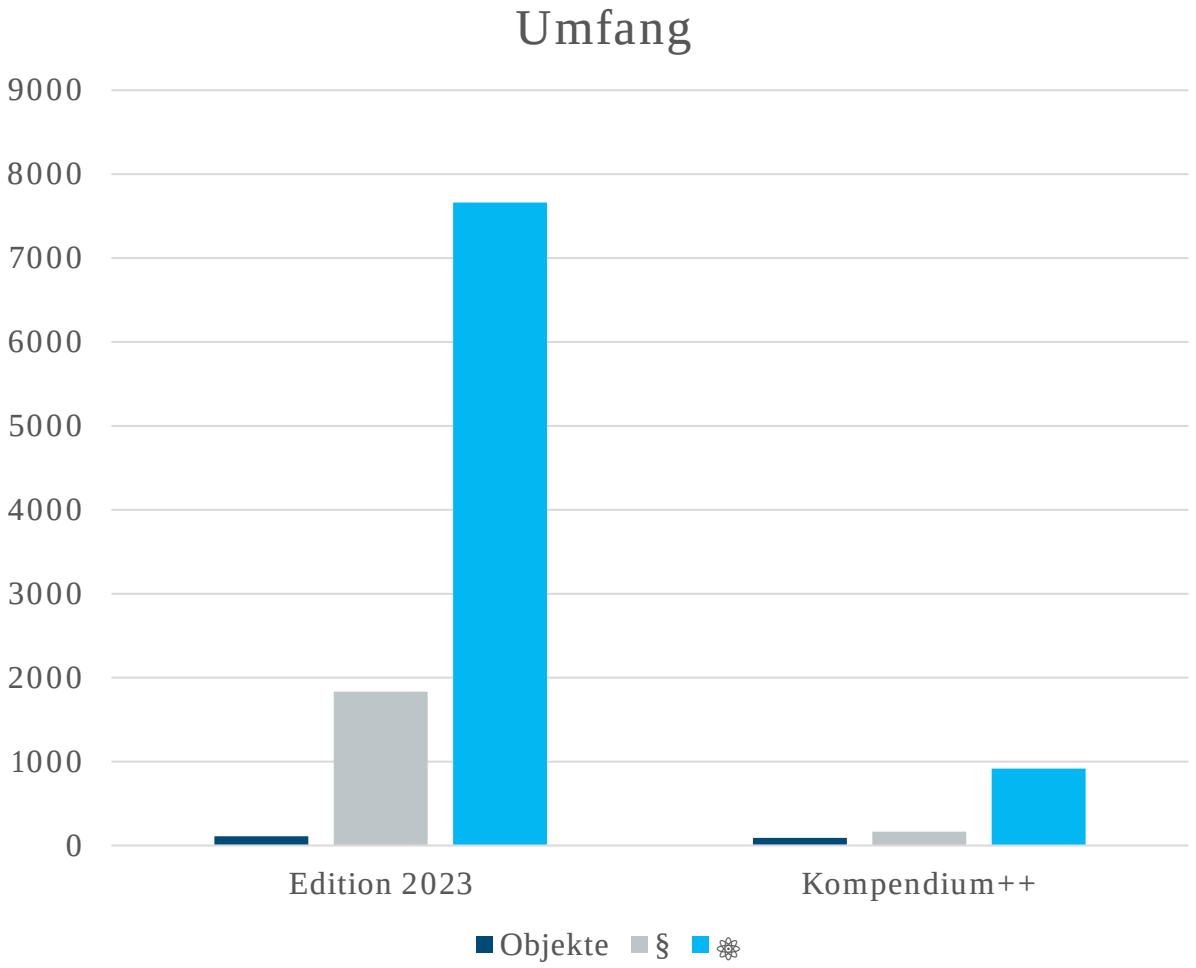
IT-Grundschutz-Vorgehensweise

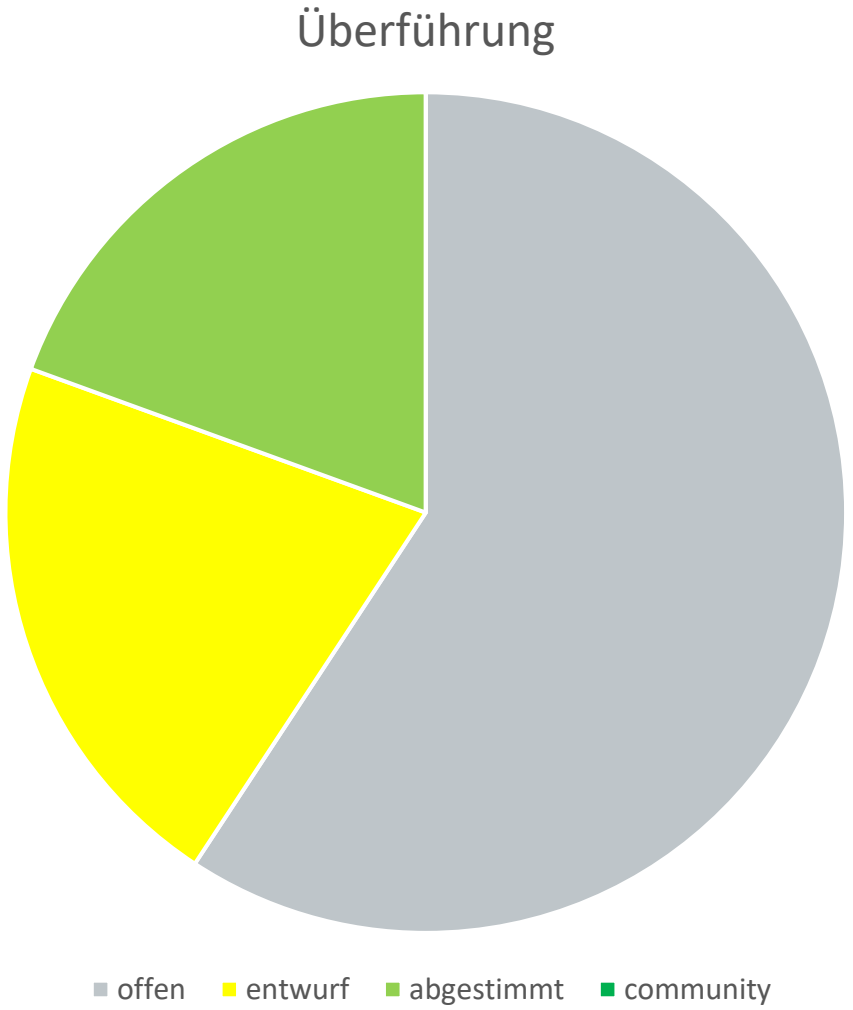
- Grundsätzliche Vorgehensweise bleibt:
  Geschäftsprozesse →
  Informationen →
  Anwendungen →
  IT-Systeme →
  Orte
- Modellierung der Anforderungen: ISMS +
  je Zielobjekt von den Blättern zur Wurzel



Sachstand

Wie viel ++ steckt schon im neuen Kompendium?

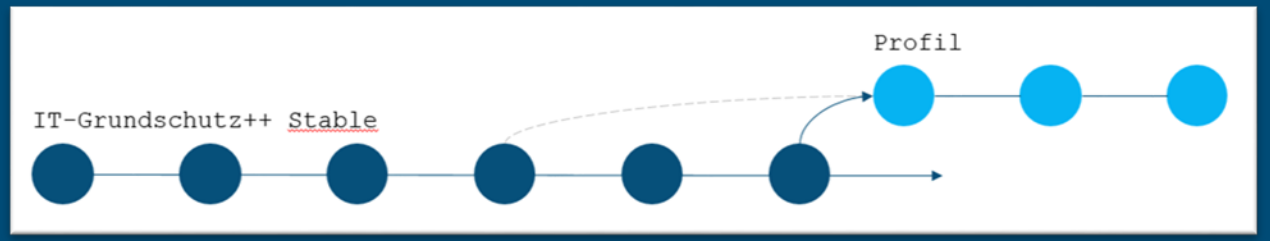


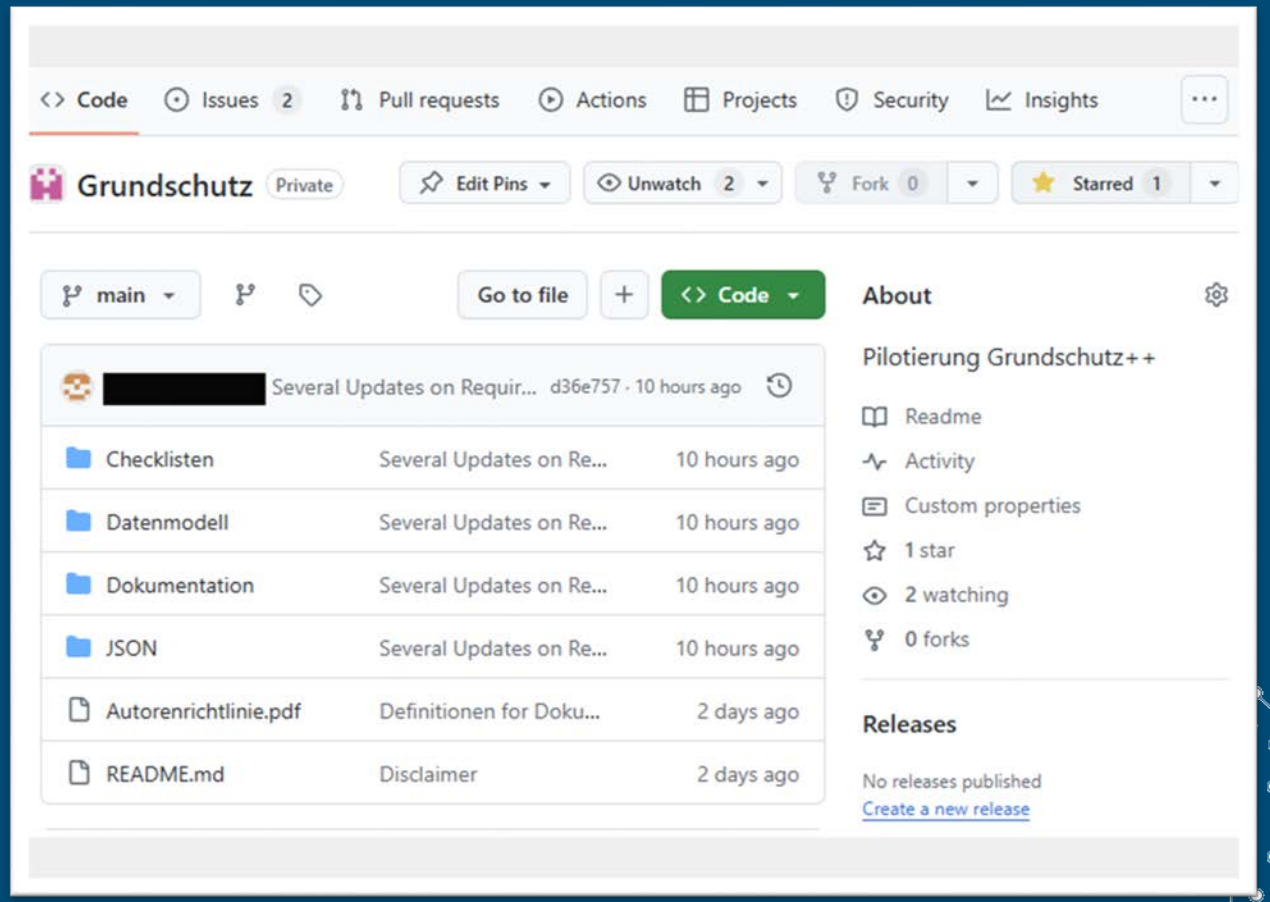


Transparenz und Engagement in der Community

Werkzeuge für jede Façon.

- **Download** in JSON und XLSX
- **Benachrichtigung** bei Änderungen per E-Mail oder Webhooks
- **Versionierung** mit Branches für Stabilität und Dynamik
- **Feedback** über Issues, Pull Requests und Discussions
- **Individualisierung** über Forks und Scripting

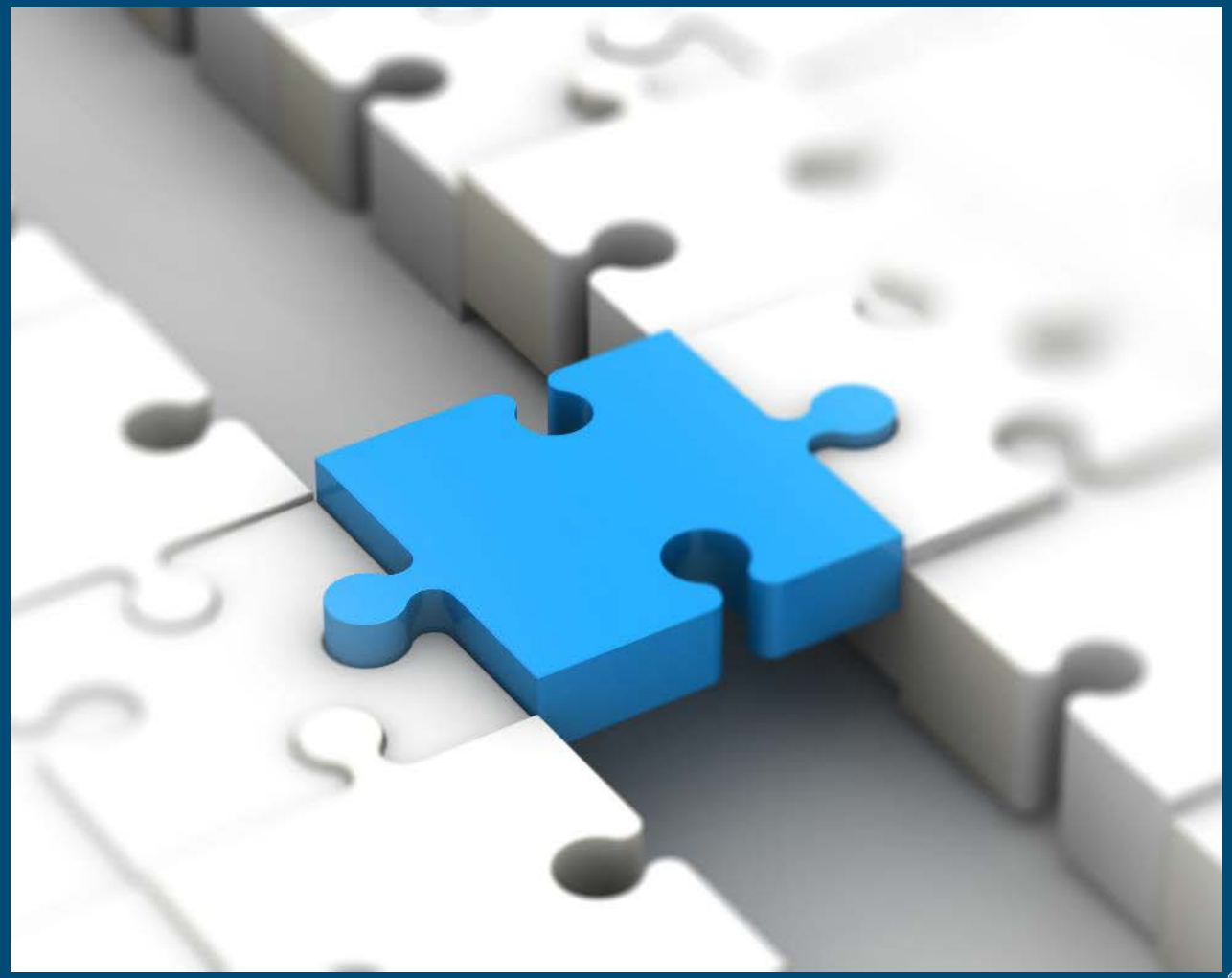




Änderungen nachverfolgen

Vereinbarkeit von Stabilität und Agilität

- UUIDs folgen **dem Inhalt**
  - Neue UUID = neue Anforderung
  - Nachverfolgbarkeit auch bei Änderungen an Text oder Fundstelle
  - Gelöschte UUID = Streichung
- gsdiff: **Vorher-Nachher** im individuellen Vergleich auf einen Blick



Mehrwert

Schneller im Ziel durch
Filtern, Automatisieren und Vereinheitlichen

Fortschritt dynamisch messen
mit Kennzahlindikatoren

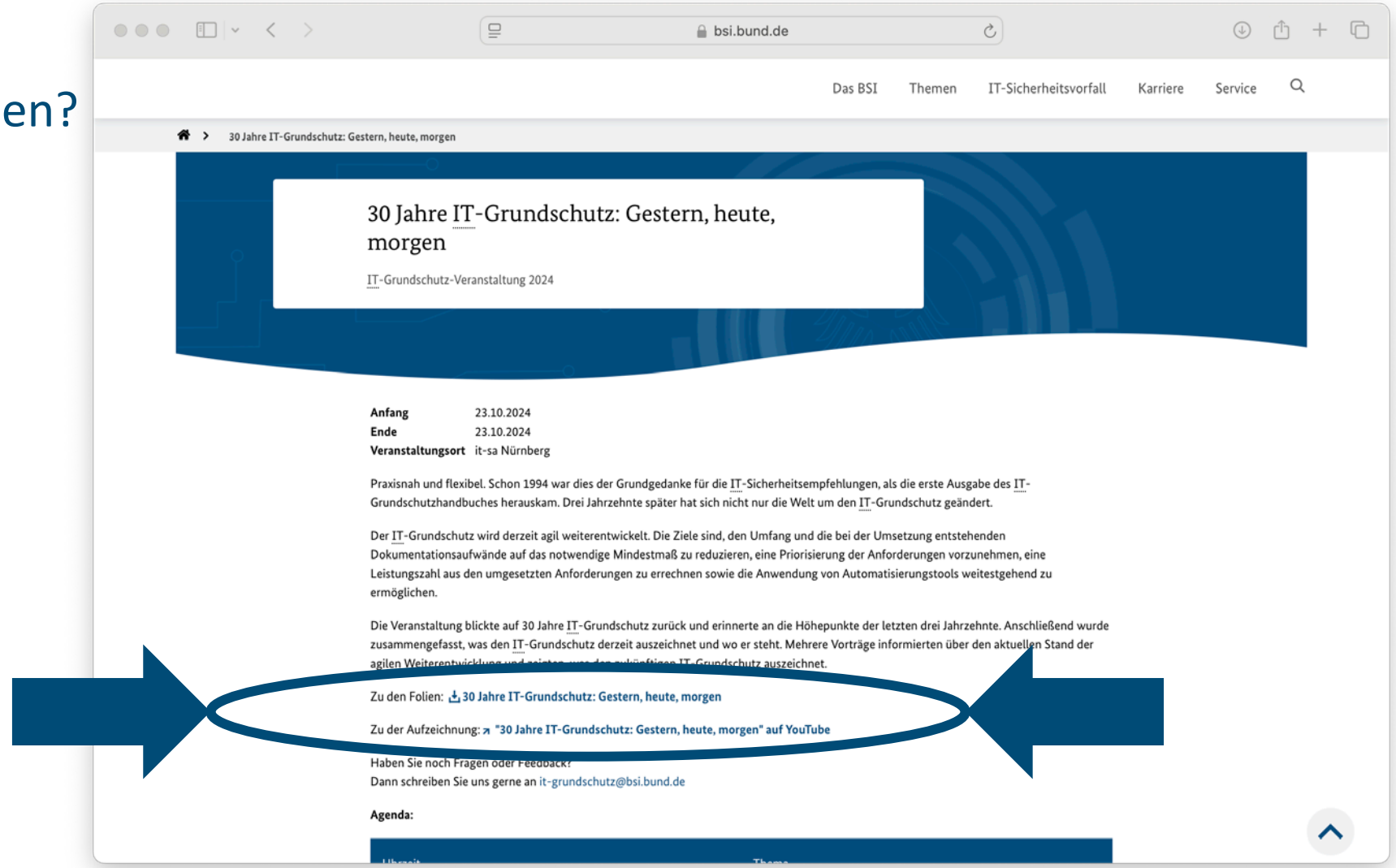
Bewährte Inhalte,
klarer formuliert und erklärt

Anpassung an
technische und rechtliche Neuerungen

Agile Veröffentlichung,
zeitnah und nachvollziehbar

Fortentwicklung IT-Grundschutz

… mehr Informationen?



https://www.bsi.bund.de/SharedDocs/Termine/DE/2024/IT_Grundschutzveranstaltung_2024.html

Fortentwicklung IT-Grundschutz

IT-Grundschutz-Kompendium 2025

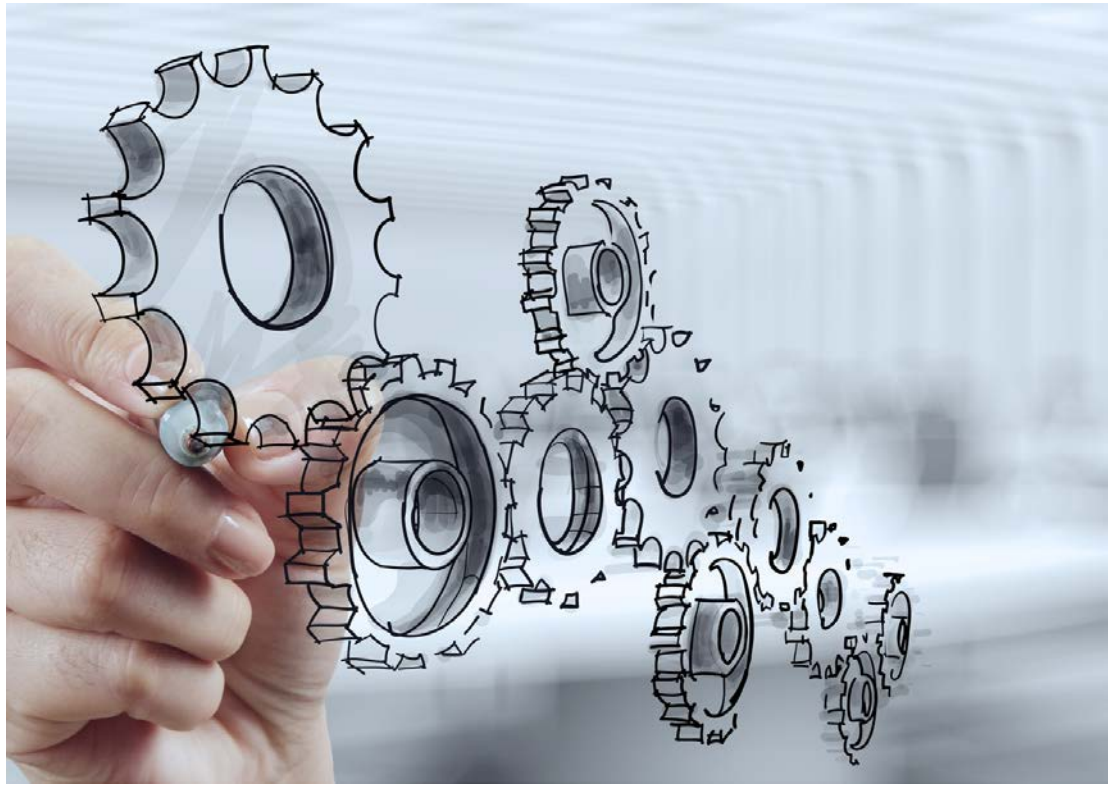
2018 bis 2023: Jährliche Veröffentlichung eines IT-Grundschutz-Kompendiums

Seit 2023: Fortentwicklung „IT-Grundschutz ++“

Auch 2025 keine Veröffentlichung einer Edition
Eventuell weitere Veröffentlichung von Community und Final Drafts

Eventuelle Fehler werden in Errata korrigiert

Keine Aufwände bei Anwendern, da nicht auf eine Edition 2025 migriert werden braucht



Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

IT-Grundschutz++ Team

it-grundschutz@bsi.bund.de
Tel.: +49 (0) 228 9582 0

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us: