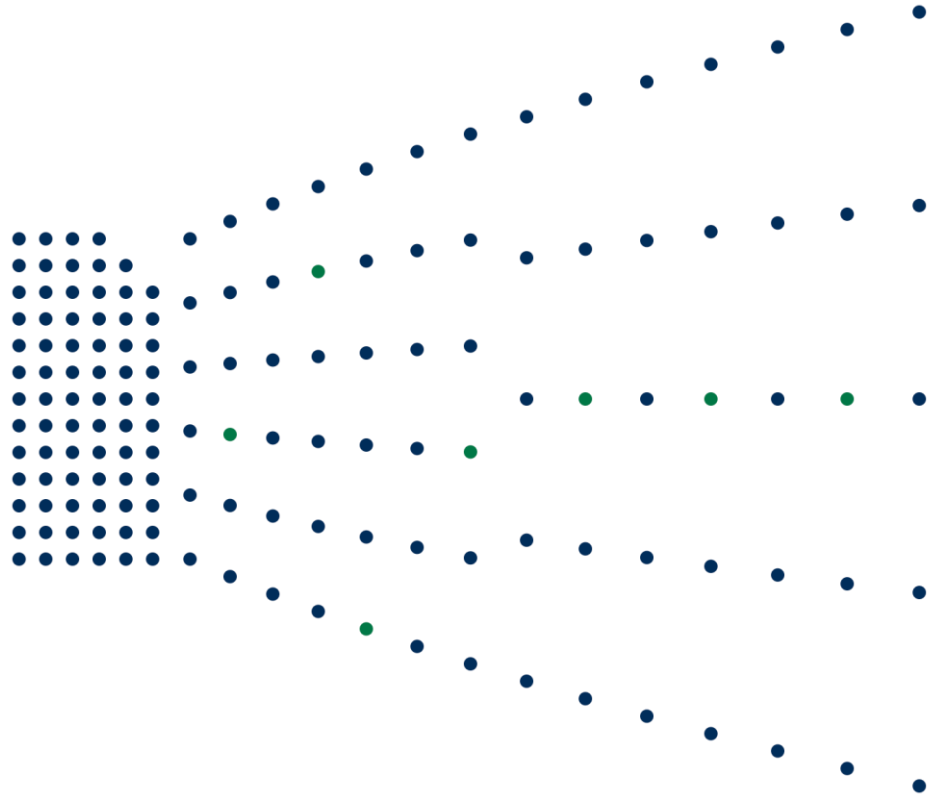
Der Anwenderkatalog nach BSI-Standard 300-1

Was drinsteht, was verloren geht, was noch fehlt

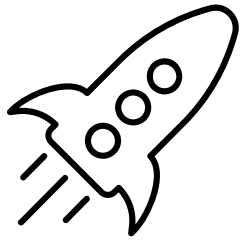
Benjamin Neweling, HiSolutions AG

Know-how to go kompakt, 16.11.2026

HISOLUTIONS



Zahlen, Daten und Fakten



Langjährige Erfahrung

Seit 1992 aktiv



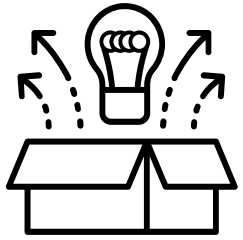
Kompetentes Personal

Mehr als 380 Beschäftigte



Kontinuierliches Wachstum

ca. 55 Mio. € Jahresumsatz



Vielfältige Kompetenzen

in mehr als 1.500 Projekten pro Jahr
bei mehr als 625 Kunden



Unsere Standorte

© HiSolutions 2026

Leistungsportfolio im Security Consulting



Penetrationstests/
Technische Audits



Cyber-Response/
Forensik



ISMS
ISO



ISMS
Grundschutz



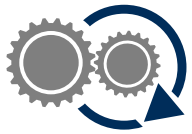
Datenschutz



Auditierung/
Zertifizierung



Sensibilisierung
und Schulung



Business
Continuity



Crisis
Management



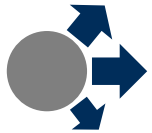
IT- Notfall-
management



Konzepte/
Risikoanalysen



Notfall- und
Krisenübungen



Third Party
Risk Management



Cloud
Security



Wirtschafts-
grundschutz



Corporate
Security



Sicherheits-
strategie



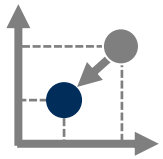
Industrial
Security



Medical
Security



Kritische
Infrastrukturen



Risk Management

© HiSolutions 2026

Benjamin Neweling berät Bundesbehörden und die Berliner Landesverwaltung zu ISMS nach IT-Grundschutz.



Benjamin Neweling

Senior Security Consultant
HiSolutions AG, Berlin

SCHWERPUNKTE

ISMS nach IT-Grundschutz

Sichere KI-Integration

Audits und Prüfungen

Mitarbeit in der Stand-der-Technik-Community
Arbeitsgruppe Risikoanalyse

VERÖFFENTLICHUNGEN

KI braucht Grundschutz
Wie (nicht nur) Behörden KI-Governance systematisch in ihr bestehendes ISMS integrieren können
<kes>, August 2026

Stichwortkommentar Digitale Sicherheit
Einträge zu ISMS und BCM
Nomos

Drei Fragen stellen sich jedem, der heute ein Sicherheitskonzept nach IT-Grundschutz pflegt.

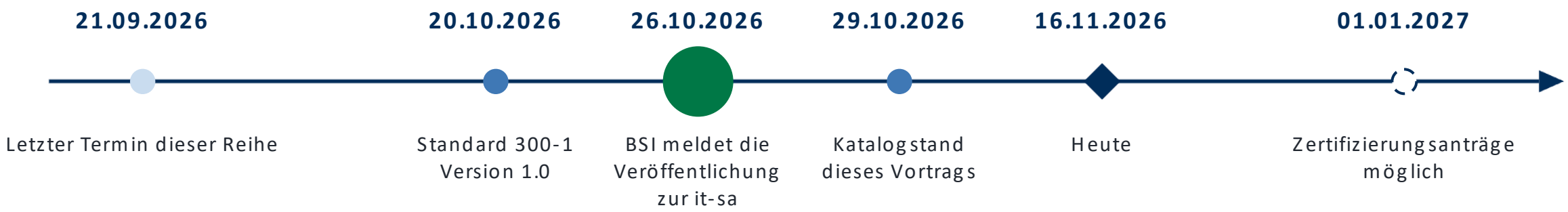
HISOLUTIONS

1 Was steht im neuen Katalog?

2 Was verliere ich gegenüber meinen Bausteinen?

3 Was fehlt noch, bis es rund ist?

Seit dem 26. Oktober gibt es zum Katalog eine verbindliche Methodik.



DIESER VORTRAG

Der Katalog

1.000 Anforderungen in 20 Praktiken, veröffentlicht in der Stand-der-Technik-Bibliothek

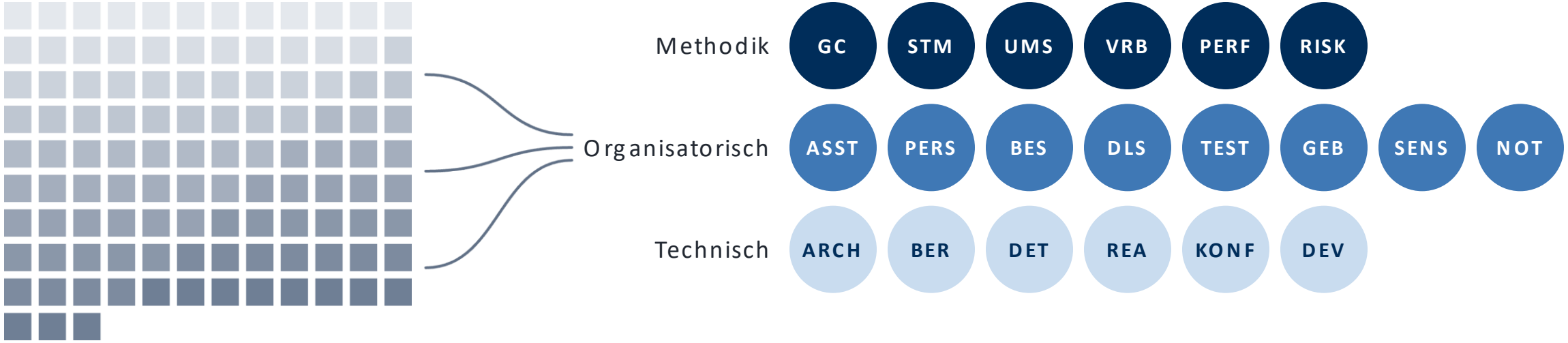
+

IM ANSCHLUSS

Die Methodik

42 Seiten BSI-Standard 300-1 mit fünf Prozessschritten

Aus 111 Bausteinen werden 20 Praktiken mit 1.000 einzeln adressierbaren Anforderungen.



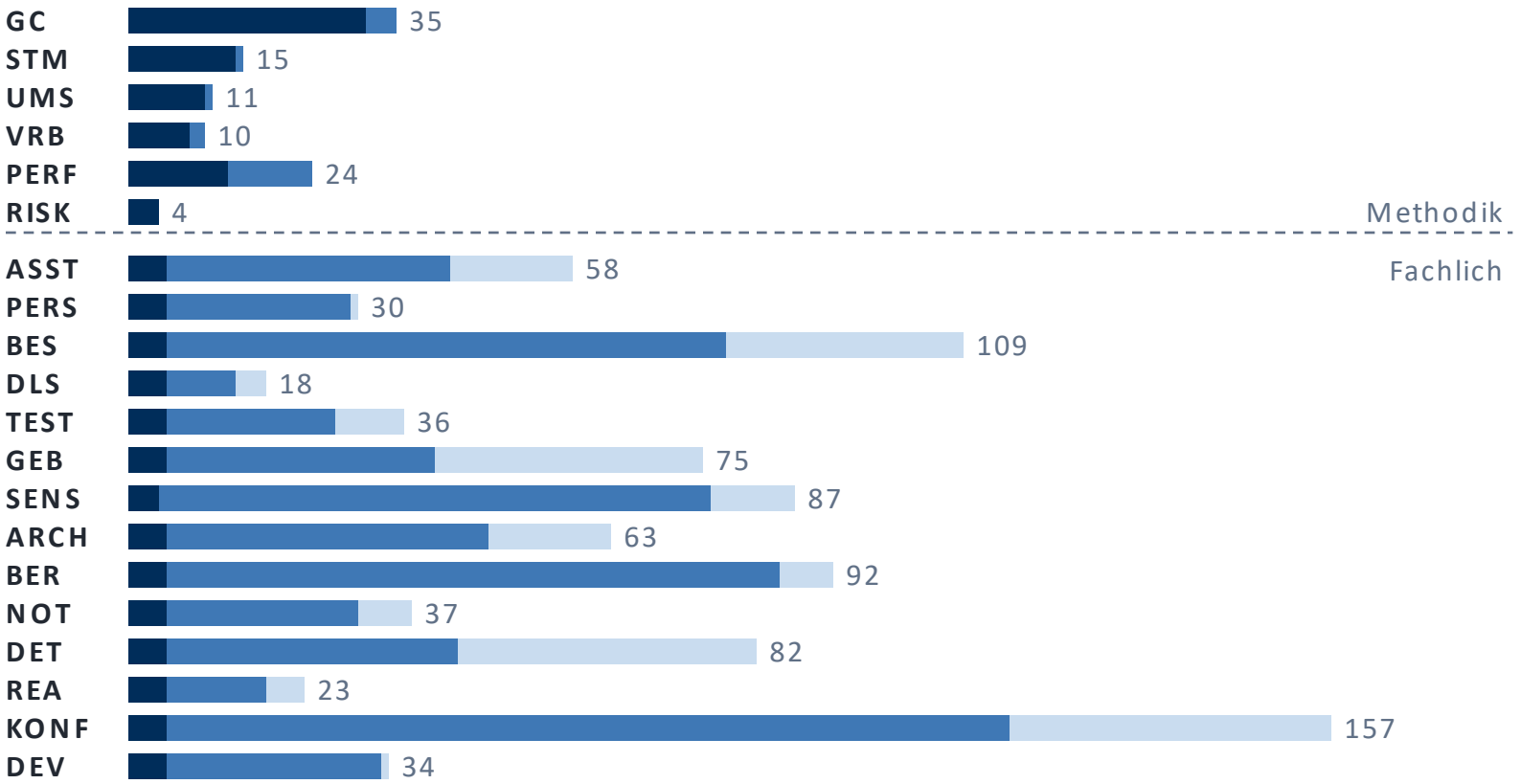
111

Bausteine in 10 Schichten, Kompendium 2023

20

Praktiken, Anwenderkatalog vom 29.10.2026

Fast jede fachliche Praktik hat genau fünf MUSS-Anforderungen. Die Substanz steht in SOLLTE.



149

MUSS-Anforderungen von 1.000

80

davon in den sechs Methodik-Praktiken

MUSS SOLLTE KANN

Jede Anforderung ist ein Satz nach Schablone und trägt ihre Einordnung als Daten mit sich.

Praktik

Modalverb. Regelt mit 300-1 die Verbindlichkeit.

Handlungswort aus fester Liste mit 27 Wörtern

Detektion SOLLTE ein zeitnahes Patchmanagement verankern.

DET.5.10 Zeitnahes Patchmanagement

EINORDNUNG ALS DATEN AN DER ANFORDERUNG

Sicherheitsniveau	Aufwand	Zielobjektkategorie	Dokumentation	Gefährdungen
normal-SdT	3 von 5	keine	Detektions-Konzept	G 0.28 und G 0.23

364 Anforderungen gelten für jeden Informationsverbund, der Rest hängt an den Zielobjektkategorien.

99

Methodik-Praktiken, immer verpflichtend

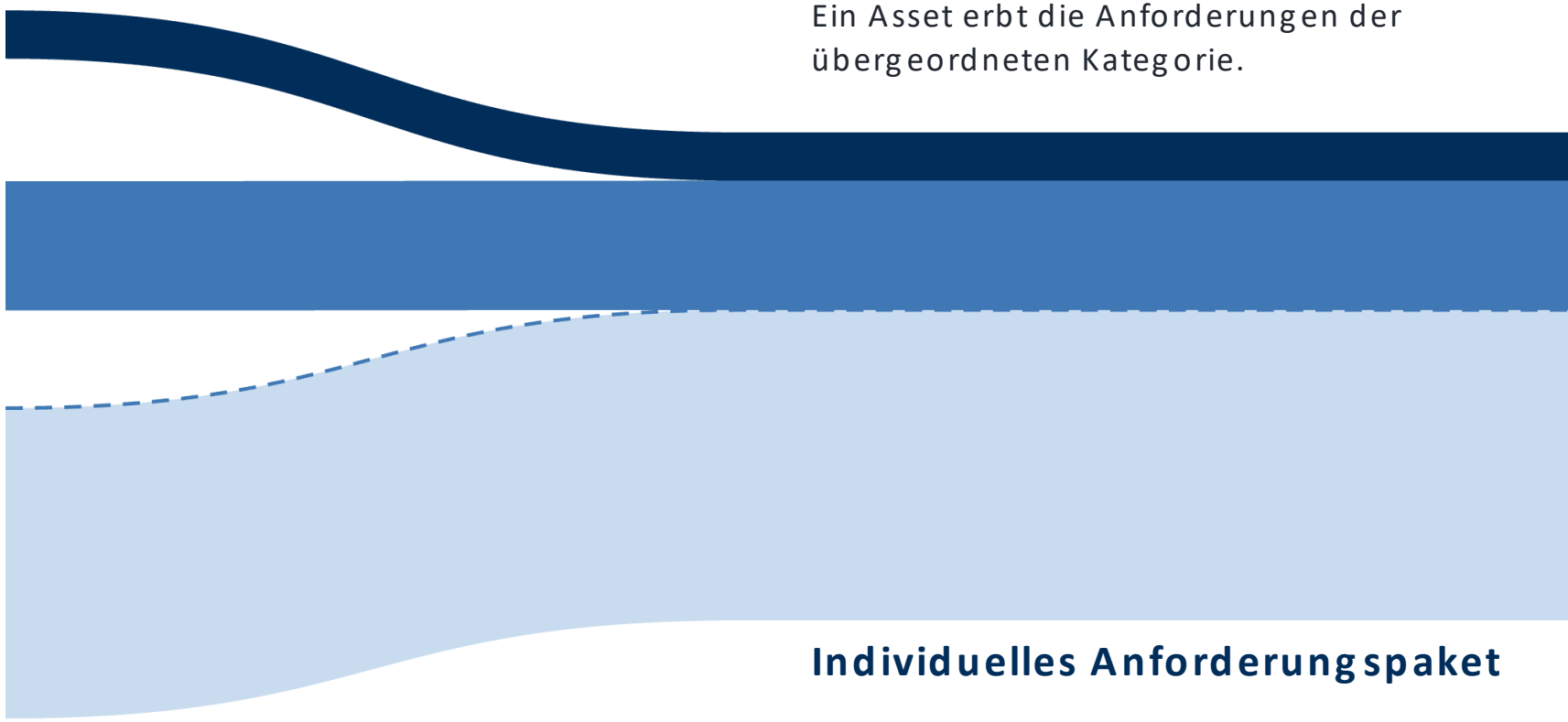
265

Fachliche Praktiken ohne Zielobjektkategorie, verpflichtend aufzunehmen

636

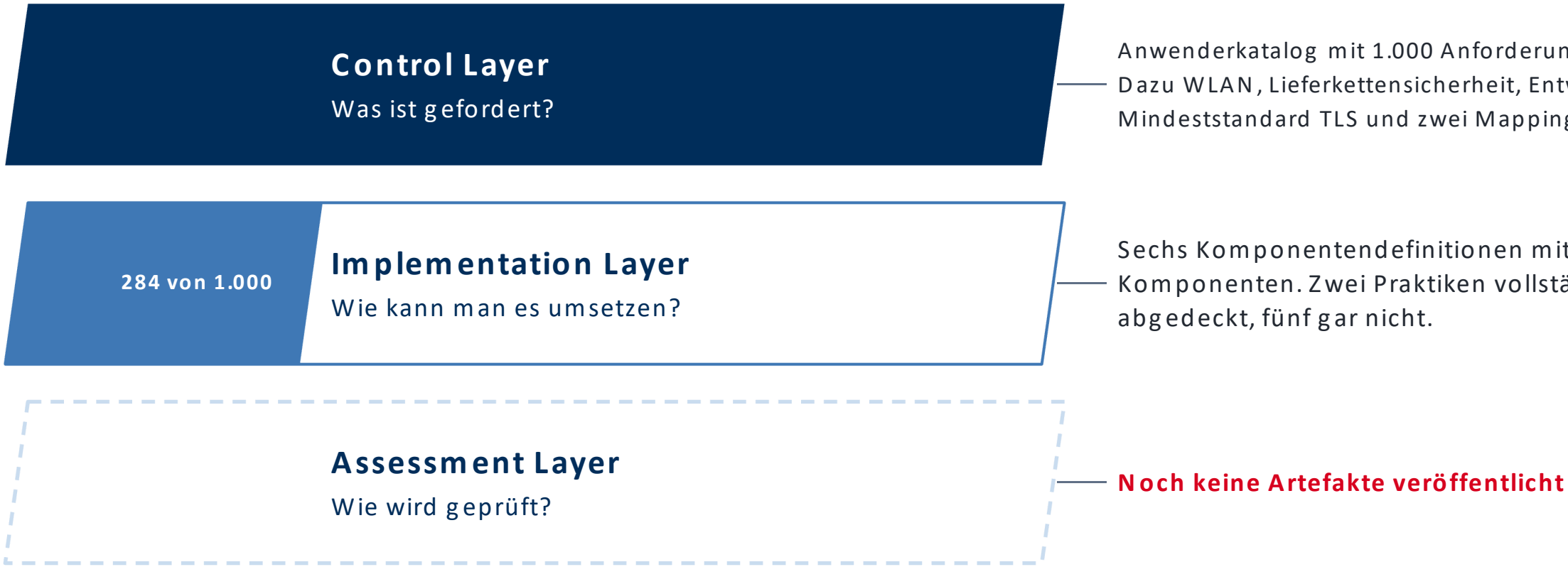
Mit Zielobjektkategorie, soweit passende Assets vorhanden sind

39 Zielobjektkategorien mit Vererbung. Ein Asset erbt die Anforderungen der übergeordneten Kategorie.

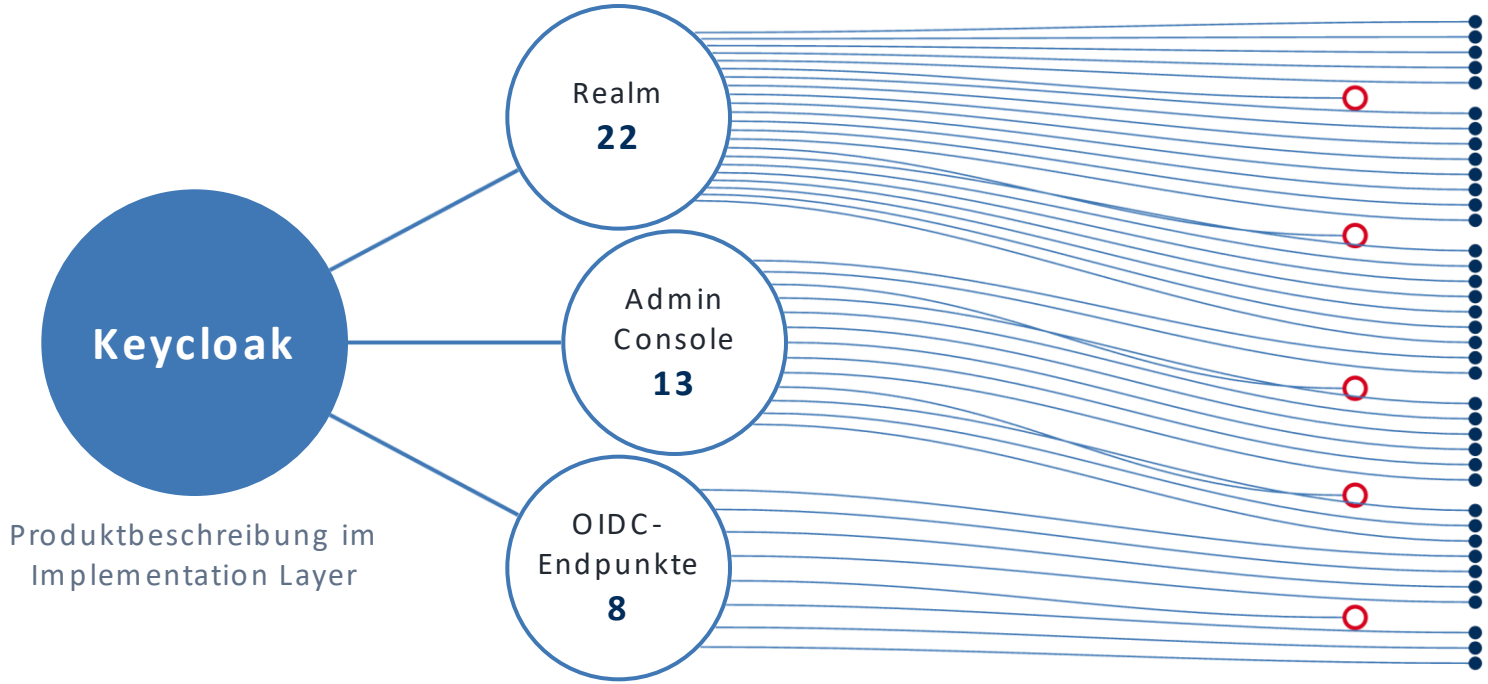


Individuelles Anforderungspaket

Die Bibliothek trennt Anforderung, Umsetzung und Prüfung. Vollständig ist bisher nur die erste Ebene.



Der Implementation Layer ist punktuell tief und in der Breite noch lückenhaft.



43 Zuordnungen zu Anforderungen aus dem Katalog

Bei 21 der 43 Zuordnungen unterstützt Keycloak nur. Konzept, Betrieb und Nachweis bleiben dort bei der Institution.

BES	DLS	ARCH	BER	DET	KONF
109 von 109	18 von 18	43 von 63	35 von 92	24 von 82	16 von 157

Was früher in einem Baustein stand, verteilt sich künftig auf drei Ebenen.



Control Layer. Abstrakte Anforderung, generische Zuständigkeit.

Implementation Layer. Produkt- und Lösungsbezug.

Assessment Layer. Prüfung.

Wer heute nur den Katalog liest, sieht die halbe Rechnung.

Ein Baustein verteilt sich auf fünf Praktiken, und Patchen gehört jetzt zur Detektion.



30 Zuordnungen im BSI-Mapping

17 Änderungen und Tests (TEST)

9 Detektion (DET)
DET.5.10 Zeitnahes Patchmanagement

2 Verbesserung (VRB)

1 Entwicklung (DEV)

1 Architektur (ARCH)

Weitere Bezüge ohne Mapping in KONF.8.2 und BES.5.10.3

Aus fünfzehn verbindlichen Aussagen in vier Basis-Anforderungen wird ein Satz mit SOLLTE.

OPS.1.1.3.A15 (B), Edition 2023

IT-Systeme und Software **SOLLTEN** regelmäßig aktualisiert werden.

Grundsätzlich **SOLLTEN** Patches zeitnah nach Veröffentlichung eingespielt werden. Basierend auf dem Konzept für das Patch- und Änderungsmanagement **MÜSSEN** Patches zeitnah nach Veröffentlichung bewertet und entsprechend priorisiert werden. Für die Bewertung **SOLLTE** geprüft werden, ob es zu diesem Patch bekannte Schwachstellen gibt. Es **MUSS** entschieden werden, ob der Patch eingespielt werden soll. Wenn ein Patch eingespielt wird, **SOLLTE** kontrolliert werden, ob dieser auf allen relevanten Systemen zeitnah erfolgreich eingespielt wurde. Wenn ein Patch nicht eingespielt wird, **MÜSSEN** die Entscheidung und die Gründe dafür dokumentiert werden.

Falls Hardware- oder Software-Produkte eingesetzt werden sollen, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, **MUSS** geprüft werden, ob diese dennoch sicher betrieben werden können. Ist dies nicht der Fall, **DÜRFEN** diese Hardware- oder Software-Produkte **NICHT** mehr verwendet werden.

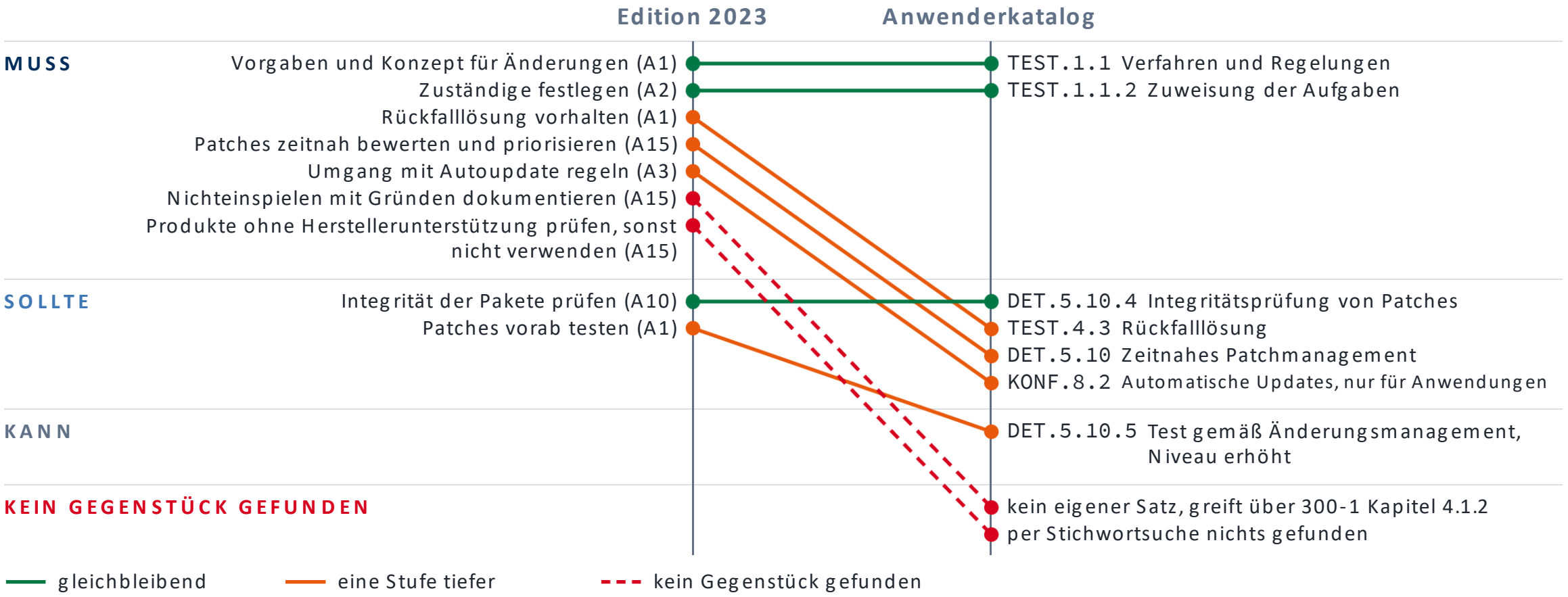
15 verbindliche Aussagen in A1, A2, A3 und A15 zusammen

DET.5.10, Katalogstand 29.10.2026

Detektion SOLLTE ein zeitnahes Patchmanagement verankern.

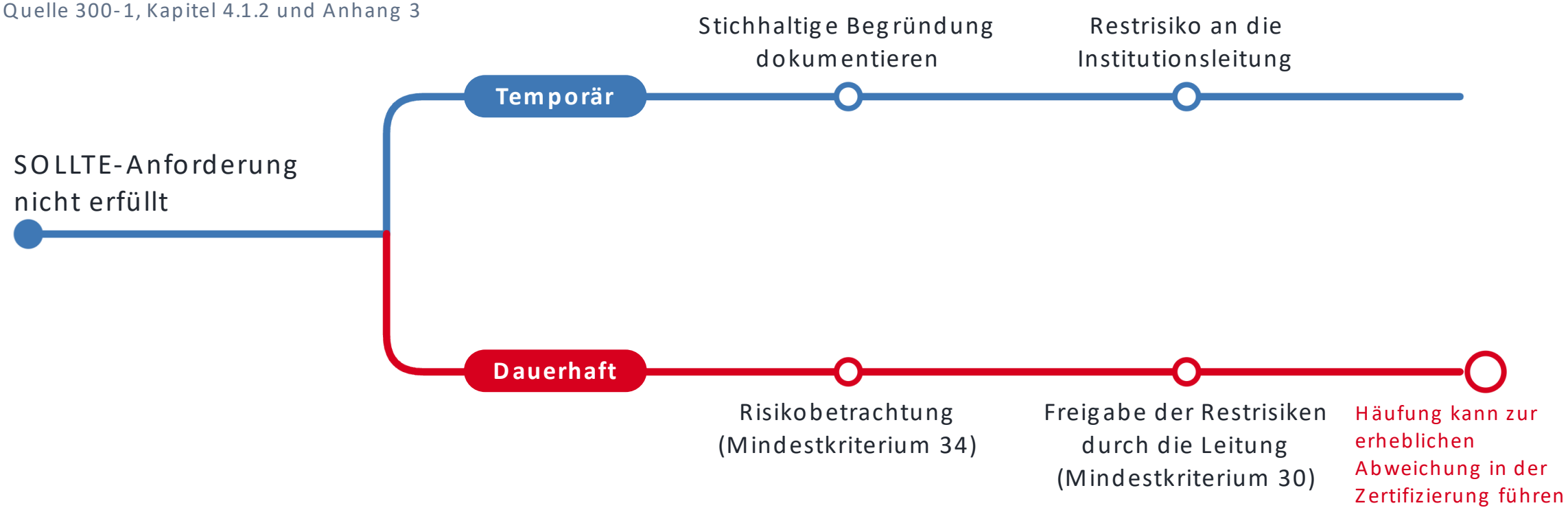
0 MUSS-Anforderungen speziell zum Patchen

Sieben von neun Pflichten haben ein Gegenstück, vier davon eine Stufe tiefer.



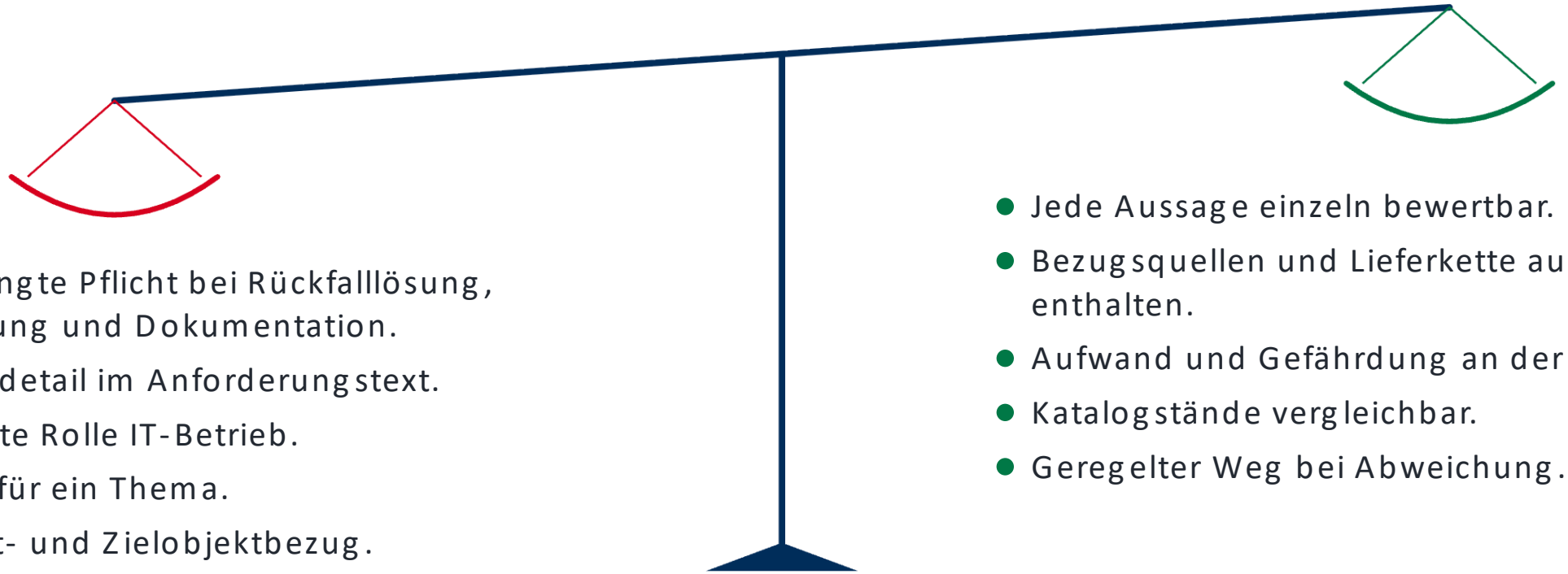
SOLLTE ist kein Freibrief, denn dauerhafte Nichterfüllung führt zwingend in die Risikobetrachtung.

Quelle 300-1, Kapitel 4.1.2 und Anhang 3



- MUSS kennt keinen Abzweig. Risikoakzeptanz und Ausnahmegenehmigung sind ausgeschlossen.

Verloren gehen Wortlaut und Bündelung, gewonnen werden Eindeutigkeit und Vergleichbarkeit.

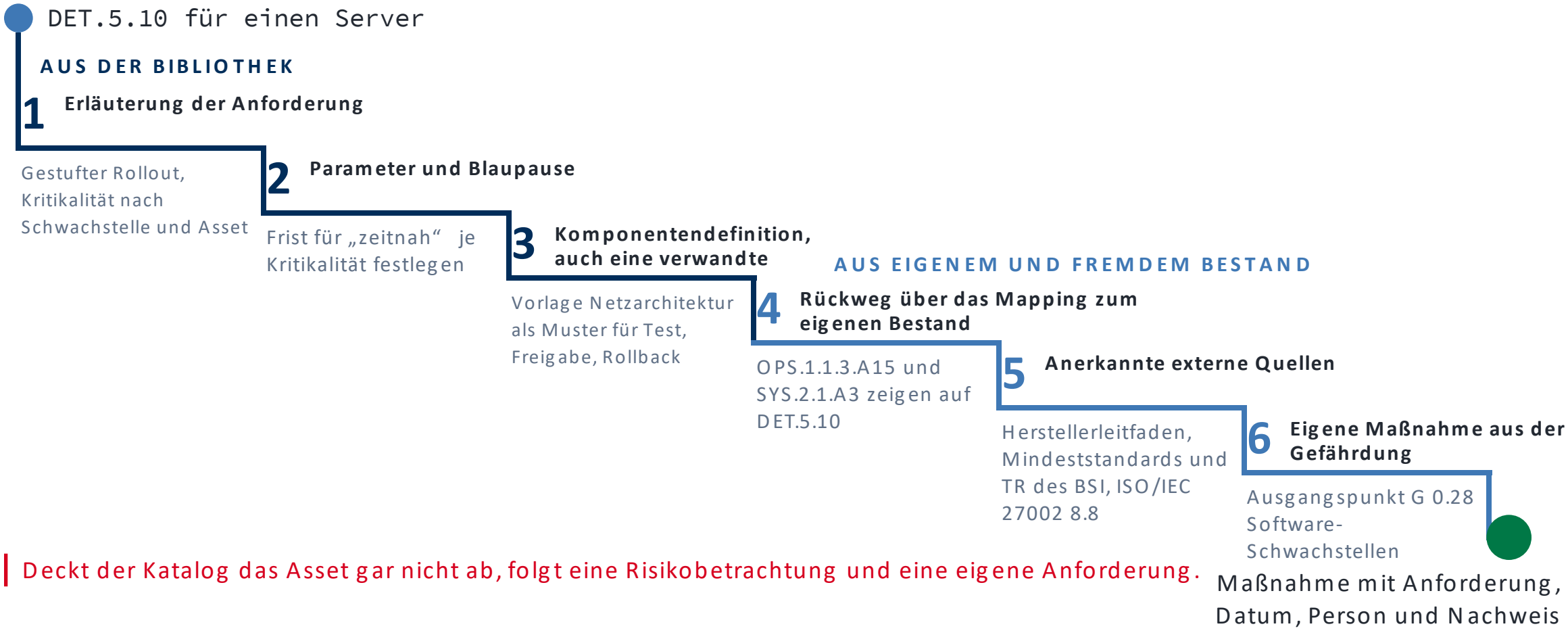


- Unbedingte Pflicht bei Rückfalllösung, Bewertung und Dokumentation.
- Prozessdetail im Anforderungstext.
- Benannte Rolle IT-Betrieb.
- Ein Ort für ein Thema.
- Produkt- und Zielobjektbezug.

- Jede Aussage einzeln bewertbar.
- Bezugsquellen und Lieferkette ausdrücklich enthalten.
- Aufwand und Gefährdung an der Anforderung.
- Katalogstände vergleichbar.
- Geregelter Weg bei Abweichung.

Beleg aus dem Implementation Layer. Die Vorlage Netzarchitektur ergänzt zu DET.5.10 bereits Test, Freigabe, Rollback und Dokumentation für Netzkomponenten.

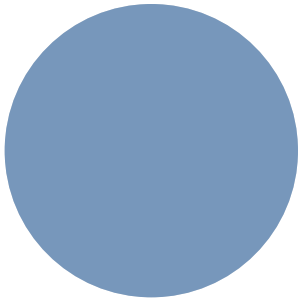
Fehlt eine Komponentendefinition, führt eine feste Reihenfolge von Quellen trotzdem zur Maßnahme.



Deckt der Katalog das Asset gar nicht ab, folgt eine Risikobetrachtung und eine eigene Anforderung.

Das BSI liefert eine maschinenlesbare Zuordnung mit vier Arten von Beziehung.

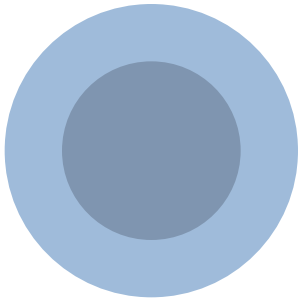
Teilanforderung Kompendium 2023 · Anforderung Grundschutz++



139

gleichwertig

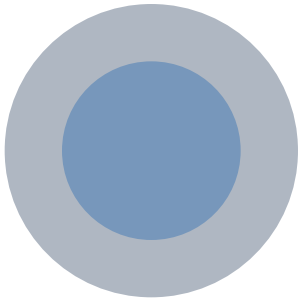
Nachweis übernehmbar



464

Alt ist Teil von Neu

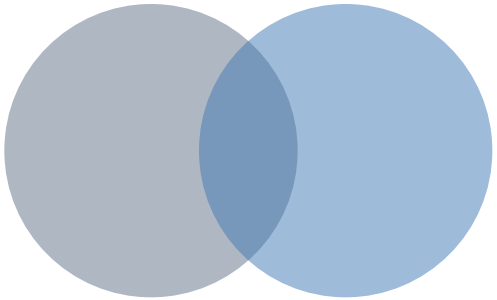
Nachweis deckt nur einen Teil



187

Alt geht über Neu hinaus

Mehrumfang fällt weg



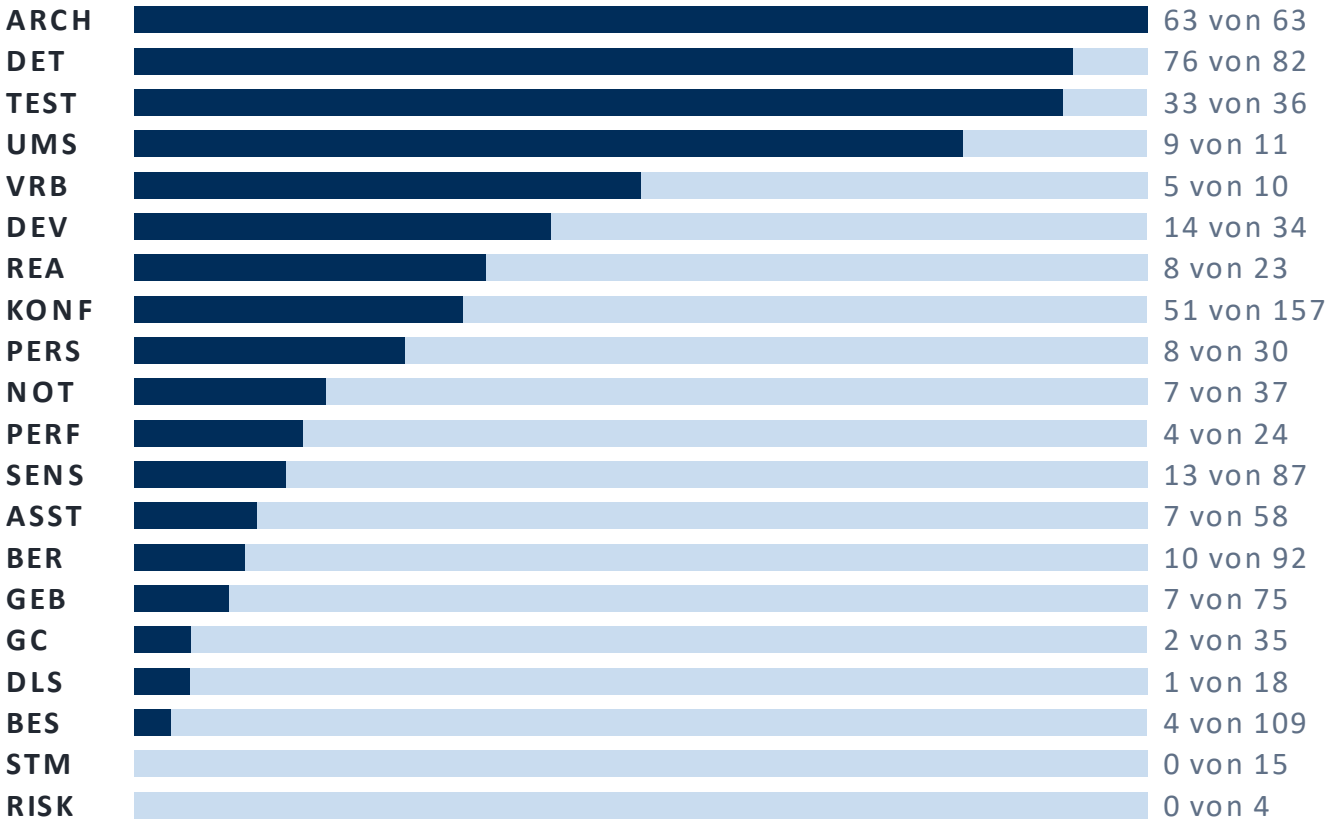
395

Überschneidung

Einzelfall prüfen

1.185 Zuordnungen. Status Entwurf, manuell erstellt, Stand 21.07.2026.

Das Mapping deckt ein Drittel des Katalogs ab und das sehr ungleich.



322

von 1.000 Anforderungen haben einen gemappten Vorgänger

510

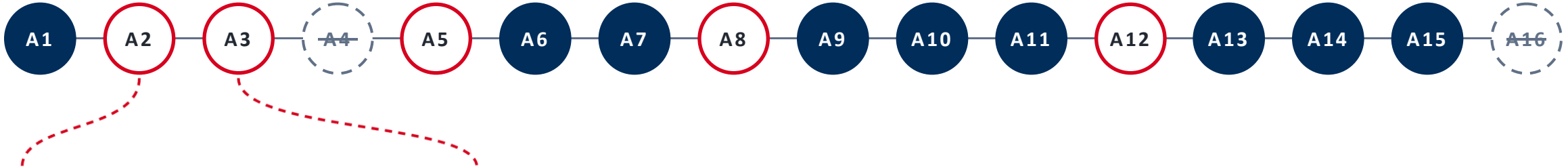
alte Anforderungen aus 94 der 111 Bausteine sind Quelle

17

Ziele des Mappings gibt es im Katalog vom 29.10. nicht mehr

„Nicht gemappt“ heißt noch lange nicht „nicht mehr gefordert“.

● 9 gemappt ○ 5 nicht gemappt ◌ 2 entfallen



A2

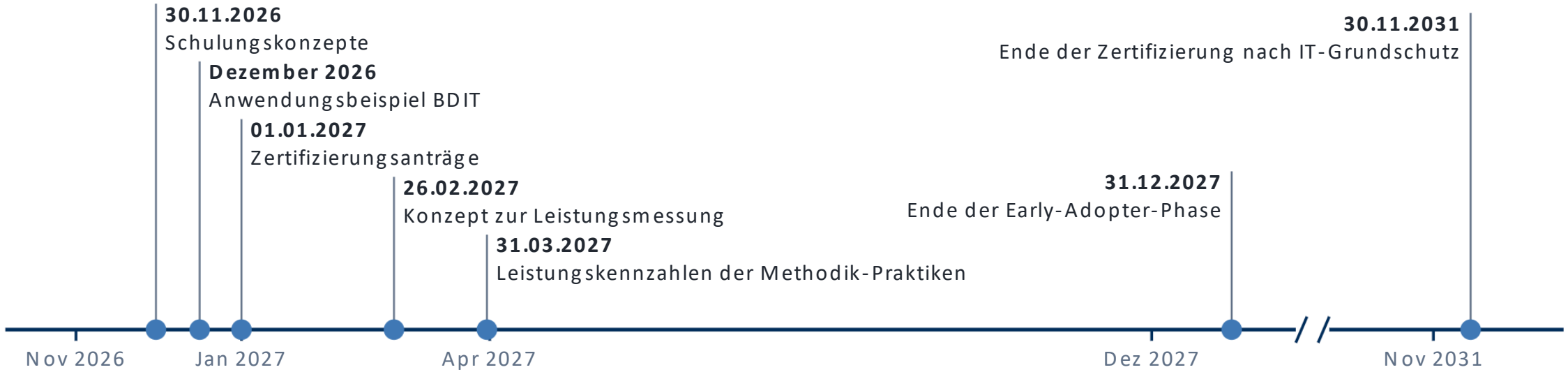
Zuständigkeiten ohne Zuordnung.
Inhaltlich nahe liegt TEST.1.1.2.

A3

Autoupdate ohne Zuordnung.
Inhaltlich nahe liegt KONF.8.2.



Sechs Lieferungen stehen noch aus, und nur für die Hälfte gibt es einen Termin.



OHNE VERÖFFENTLICHTEN TERMIN

- Implementation Layer für alle Praktiken
- Assessment Layer und Prüfvorgaben
- Finales Mapping zum aktuellen Katalog

Meilensteinplan des BSI, Stand Oktober 2026, ausgewertet über Sekundärquellen

Der Standard beschreibt den Neuaufbau, der Umstieg bleibt Aufgabe der Anwender.

Zum Umstieg vom Kompendium sagt 300-1 **nichts** .

Volltextsuche im Standard

Die Leistungsbewertung dürfen Institutionen vorerst **frei** gestalten.

Kapitel 5.1

Der Umsetzungsstatus kennt kein **teilweise** mehr.

Kapitel 4.1.1

Geänderte Katalogstände lösen eine **Validierung** der Anforderungen aus.

Kapitel 5.5

Fünf Schritte lohnen sich jetzt, auch wenn der Umstieg erst in Jahren ansteht.



Wer seine heutige Umsetzung sichert, verliert beim Umstieg wenig.

HISOLUTIONS

Der **Katalog** sagt, was erreicht werden soll.

Das **Wie** liegt künftig auf Ebenen, die erst für einzelne Themen gefüllt sind.

SOLLTE verlangt eine begründete Entscheidung und bei Verzicht eine Risikobetrachtung.

Interesse geweckt?
Ausbildungen der HiAcademy

Die **HiAcademy** bietet strukturierte Ausbildungen rund um IT-Grundschutz und ISMS an

01 **Ausbildung zum IT-Grundschutz-Praktiker**

Einstieg in die Umsetzung – praxisnah, mit BSI-Zertifizierung

02 **Ausbildung zum IT-Grundschutz-Berater**

Vertiefung und Zertifizierung für erfahrene Praktiker

hisolutions.com/hiacademy

academy@hisolutions.com