BlueProceedings ISMS

Grundschutz++ · BSI-Standard 300-1, Kap. 2

Prozessschritt 1 im Detail.

Alle elf Teilschritte. Je Folie: was der Standard verlangt, und wie wir es interpretieren.

Wie viele Entscheidungen sind bei euch nur noch „historisch gewachsen“?

1 Erhebung und Planung

2 Anforderungs-analyse

3 Realisierung

4 Überwachung

5 Kontinuier-liche Verbesserung

Teil 3 der Beitragsreihe · Wischen →

02 KAPITEL 2 AUF EINEN BLICK

Elf Teilschritte, vier im Fokus.

Die ersten vier klären, bevor die erste Maßnahme entsteht: Was wirkt auf uns? Was müssen wir einhalten? Wofür gilt das ISMS? Wer erwartet was?

2.1 Folien 3–7
Kontext
Was wirkt auf uns?

2.2 8–10
Compliance
Was müssen wir einhalten?

2.3 11
Anwendungs-bereich
Wofür gilt das ISMS?

2.4 12–13
Interessierte Parteien
Wer erwartet was?

2.5 14
Geschäftsprozesse
Was tun wir?

2.6 14
Schutzbedarf
Normal oder hoch?

2.7 15
Leitlinie
Wohin wollen wir?

2.8 15
Rollen
Wer macht was?

2.9 15
Dokumentation
Was gilt, wer weiß es?

2.10 16
Freigabe
Wer entscheidet?

2.11 16
Risikorahmen
Wie viel Risiko tragen wir?

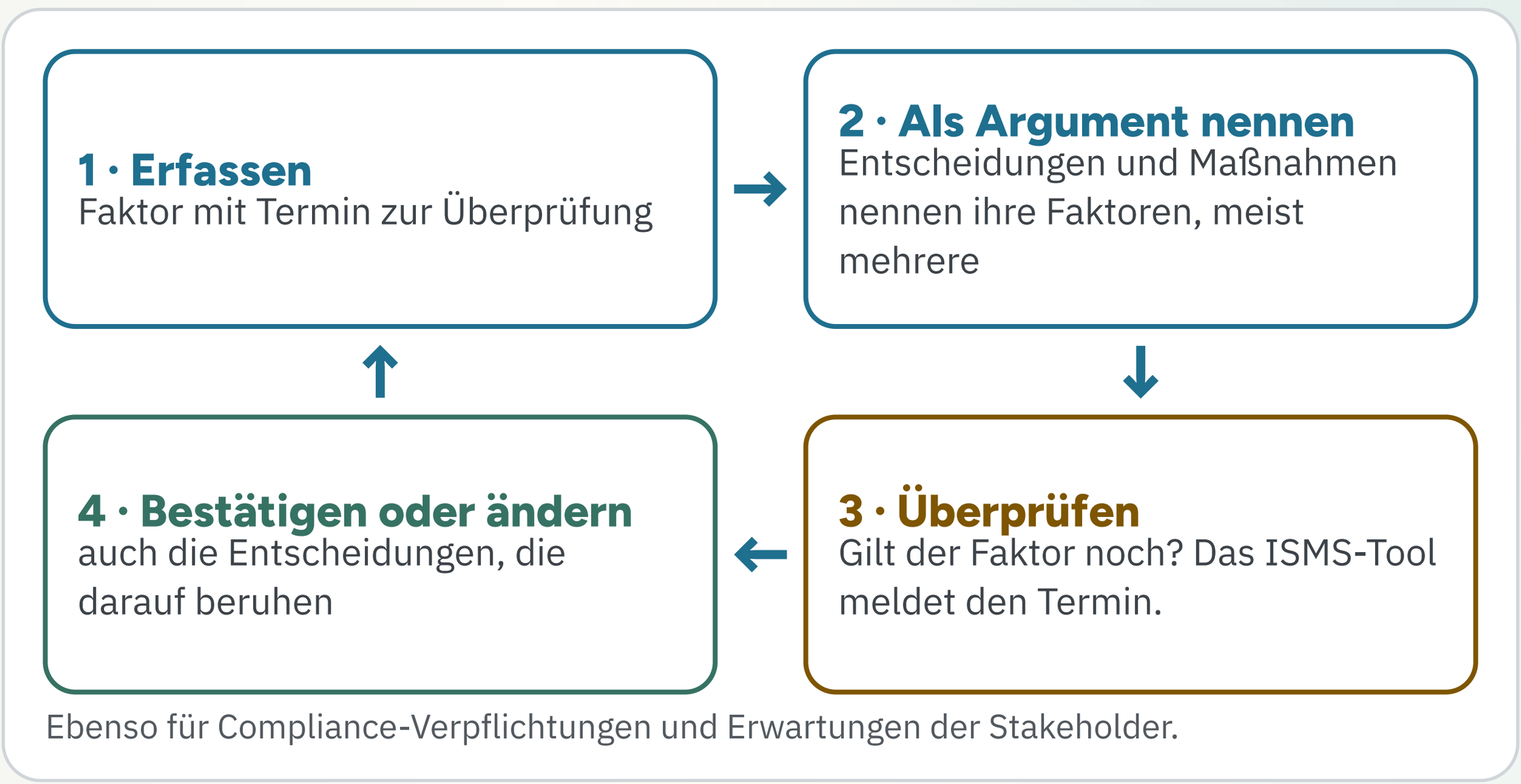
Folie 17
Alles zusammen an einem Prozess

03 2.1 · KONTEXT

Vom Faktor zur Überprüfung.

BSI-STANDARD 300-1 VERLANGT
Die Faktoren erfassen, die extern (z. B. NIS-2, Bedrohungslage, Lage am Fluss) und intern (z. B. Strategie, Kultur, Ressourcenmangel) auf die Institution wirken, und **knapp** festhalten, welche das ISMS prägen.

BEI BLUEPROCEEDINGS ISMS
Knapp ja, aber verbunden. Ein Faktor, der nur in einer Liste steht, erklärt später keine Entscheidung.

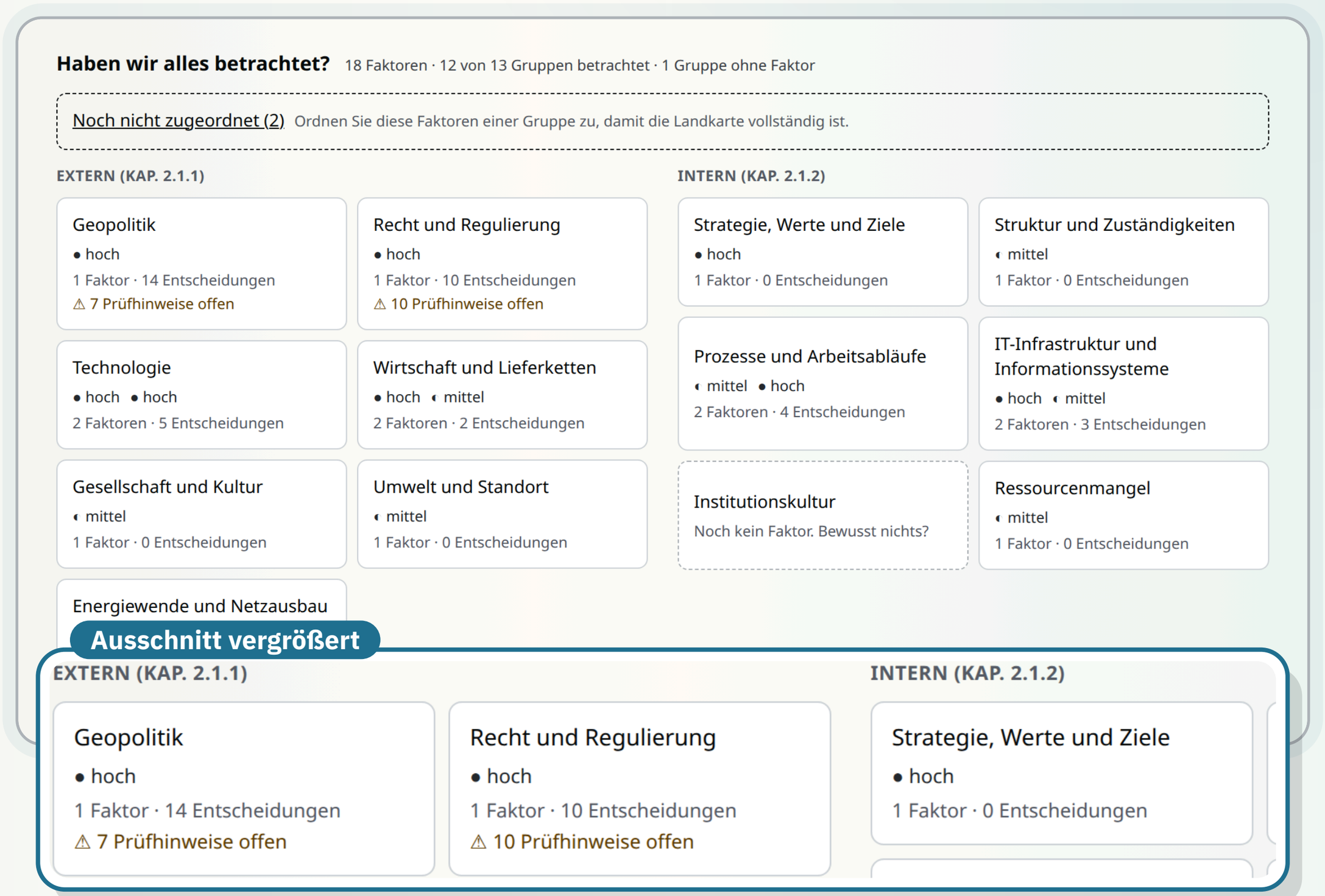


Ebenso für Compliance-Verpflichtungen und Erwartungen der Stakeholder.

Haben wir alles betrachtet?

BSI-STANDARD 300-1 VERLANGT
Unter anderem diese Gruppen berücksichtigen: extern Geopolitik, Recht, Technologie, Wirtschaft, Gesellschaft, Umwelt; intern Strategie, Struktur, Prozesse, IT, Kultur, Ressourcen.

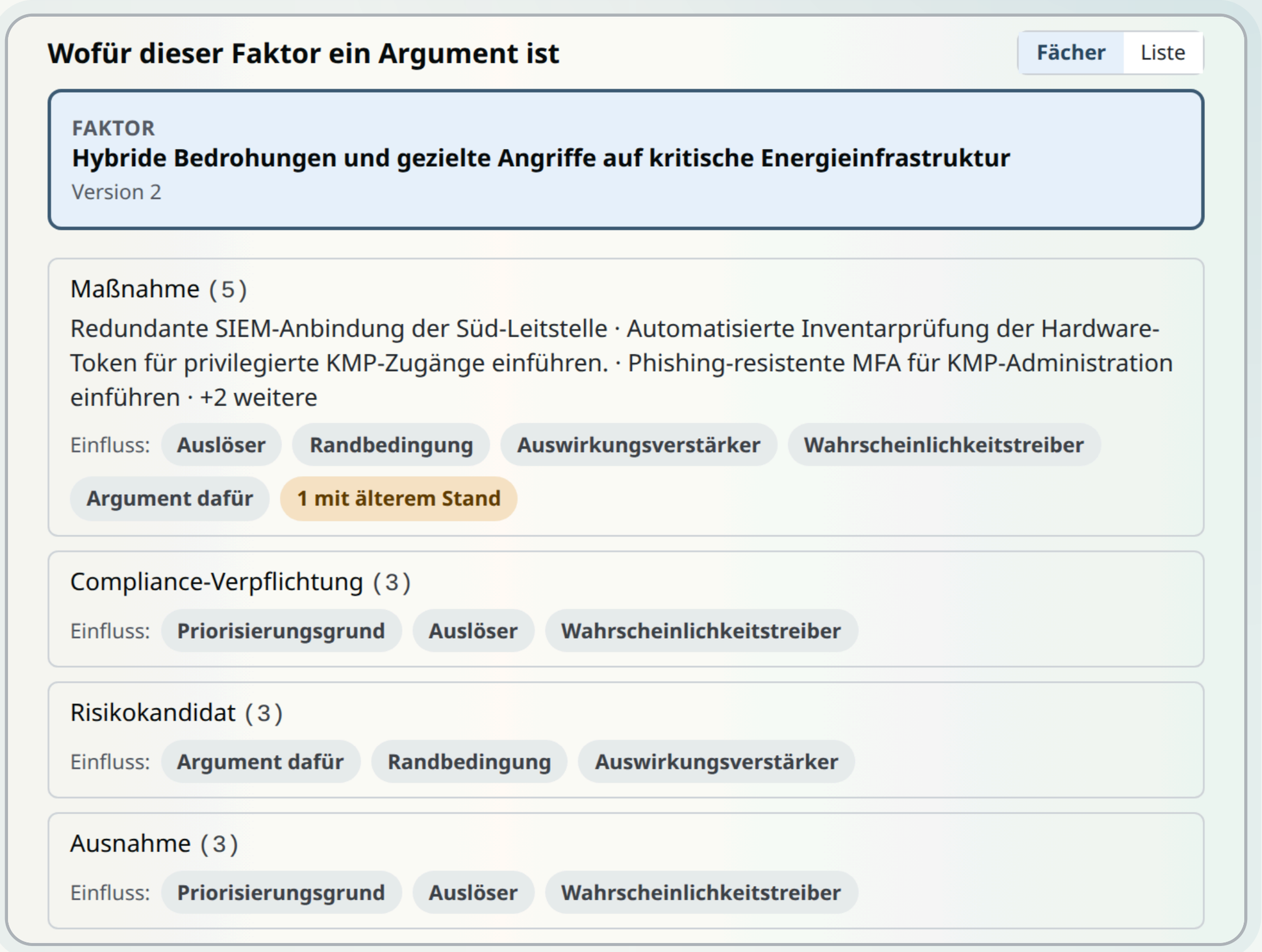
BEI BLUEPROCEEDINGS ISMS
Jeder Faktor gehört zu einer Gruppe, den Gruppen des Standards oder eigenen. Die Übersicht zeigt, wozu noch nichts erfasst ist. Eingeordnet wird nichts automatisch.



Ein Faktor, viele Entscheidungen.

Unsere Interpretation · keine Vorgabe des Standards

Zu jedem Faktor zeigt das ISMS-Tool, welche Entscheidungen und Maßnahmen ihn als Argument nennen, und welche Rolle er dort spielt: Auslöser, Randbedingung, Argument dafür und mehr.



„Mit älterem Stand“ heißt: Die Entscheidung nennt noch eine frühere Fassung des Faktors.

Hat sich etwas verändert?

Unsere Interpretation · keine Vorgabe des Standards

Ein Faktor kann an eine KPI gebunden sein, hier die Zahl überfälliger Maßnahmen. Nennt eine Entscheidung den Faktor, bleibt der damalige Wert festgehalten.

Wie hat sich die KPI „Überfällige Maßnahmen“ seit den Entscheidungen verändert? Heute: 7 Maßnahmen

Der Faktor **Rückstau bei überfälligen Maßnahmen** ist an eine KPI aus den Daten dieser Anwendung gebunden. Maßnahmen mit überschrittener Frist, die weder abgeschlossen noch zurückgestellt noch nur eine Idee sind. Beim Bezug einer Entscheidung auf den Faktor wird die Zahl festgehalten; hier steht sie neben dem heutigen Wert.

Redundante SIEM-Anbindung der Süd-Leitstelle

4 bei Entscheidung (2026-10-31) → 7 heute (+3)

Lieferantenrollen rezertifizieren

5 bei Entscheidung (2026-10-31) → 7 heute (+2)

Zweiten Collector bereitstellen und automatischen Failover testen.

6 bei Entscheidung (2026-10-31) → 7 heute (+1)

- ○ Wert bei der Entscheidung, ● Wert heute.
- Eine gestiegene Zahl ist Anlass, den Faktor erneut zu prüfen.
- Das Tool bewertet die Abweichung nicht. Ob neu entschieden wird, entscheiden die Zuständigen.

07 2.1 · 2.2 · 2.4

Was steht in den nächsten 90 Tagen an?

Unsere Interpretation · keine Vorgabe des Standards

Faktoren, Stakeholder und Compliance-Verpflichtungen haben Termine zur Überprüfung. Das ISMS-Tool sammelt sie an einer Stelle, nach überfällig und Zeitraum.

WAS STEHT IN DEN NÄCHSTEN 90 TAGEN AN? ■ 1 überfällig

Überprüfungen, Fristen und Abläufe von Faktoren, Stakeholdern und Compliance-Verpflichtungen. Die Ansicht liest nur; Aufgaben entstehen im Tageslauf.

Band | Liste

	Überfällig	Heute bis 30 Tage	31 bis 60 Tage	61 bis 90 Tage
Faktoren				• fällig 15.01.2027 Überprüfung: Lieferkettenlage bei Mikrochips und Steuerungskomponenten • fällig 29.01.2027 Überprüfung: Rückstau bei überfälligen Maßnahmen • fällig 29.01.2027 Überprüfung: Zuständigkeiten für einzelne Anwendungen nicht durchgängig geregelt
Stakeholder				
Compliance-Verpflichtungen	■ **überfällig 19.10.2026** Überprüfung: EnWG/MsbG-Marktkommunikation	• fällig 28.11.2026 Überprüfung: DSGVO	• fällig 15.12.2026 Überprüfung: Verfügbarkeitszusage Fernwärme-Großabnehmer • fällig 28.12.2026 Überprüfung: Berichtspflicht Informationssicherheit an den Aufsichtsrat • fällig 30.12.2026 Überprüfung des Rechtskatasters: Rechtskataster	• fällig 15.01.2027 Frist: Verfügbarkeitszusage Fernwärme-Großabnehmer • fällig 15.01.2027 Überprüfung: Meldung von Sicherheitsvorfällen an den Netzbetreiber binnen 24 Stunden

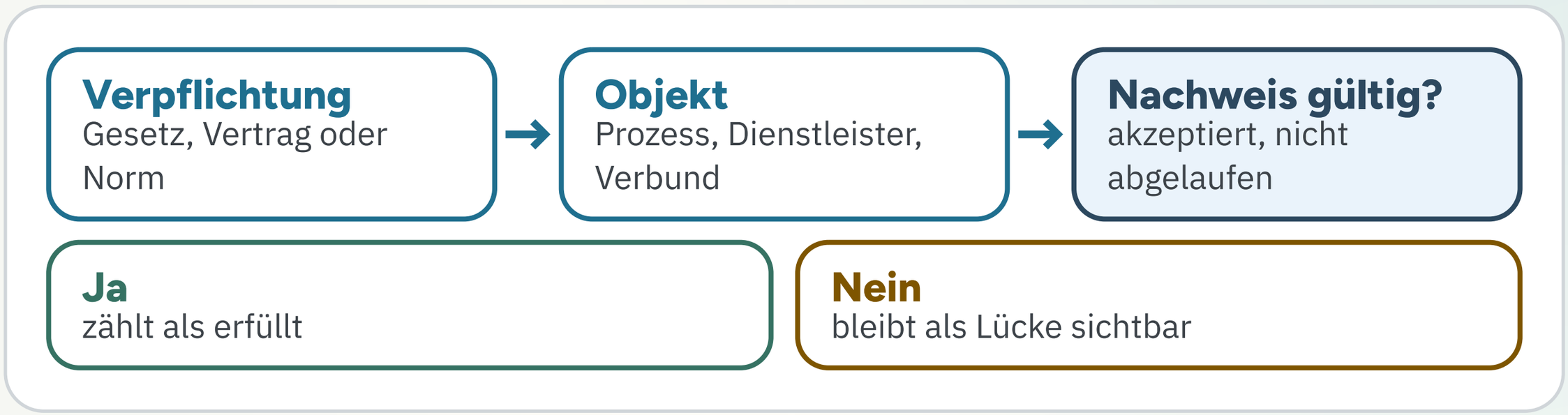
■ überfällig, • fällig. Grundlage: BSI-Standard 300-1, Kap. 2.1 und 2.4 (regelmäßige Überprüfung).

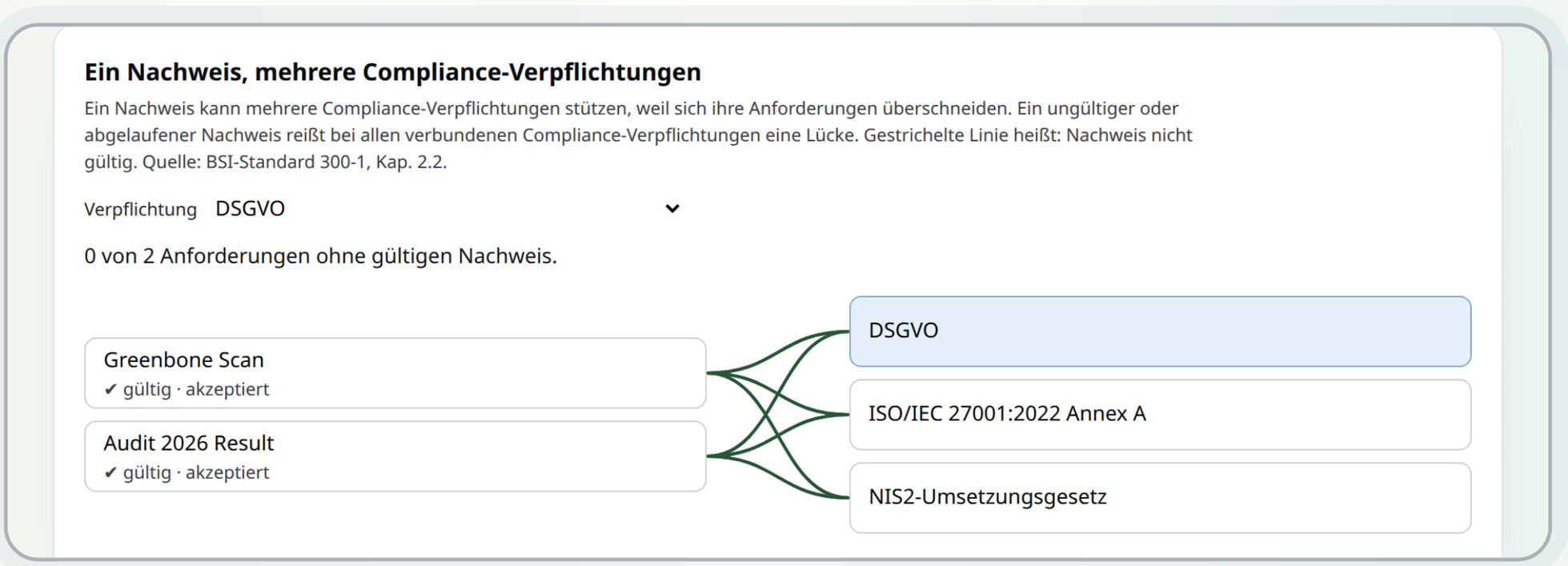
08 2.2 · COMPLIANCE

Ohne Nachweis nicht erfüllt.

BSI-STANDARD 300-1 VERLANGT
Gesetze, Verträge, interne Regelwerke und Anforderungskataloge analysieren; gesetzliche und vertragliche Verpflichtungen dokumentieren. Ihre Anforderungen fließen ins Anforderungspaket.

BEI BLUEPROCEEDINGS ISMS
Jede Compliance-Verpflichtung steht neben den Objekten, für die sie gilt. Erfüllt ist sie dort nur mit gültigem Nachweis.





Ein Nachweis kann mehrere Verpflichtungen stützen. Wird er ungültig, fällt er bei allen weg.

09 2.2 · COMPLIANCE

Wo gilt welche Compliance-Verpflichtung?

Unsere Interpretation · keine Vorgabe des Standards

Je Verpflichtung und Objekt zeigt die Matrix, wie viele Anforderungen umgesetzt sind. Ein Strich heißt: gilt hier nicht.

Wo gilt welche Compliance-Verpflichtung, und wie weit sind wir?

Eine Verpflichtung gilt für die Objekte, die über Prozesse, Dienstleister und Schnittstellen erreicht werden. „–“ heißt: gilt hier nicht. „nicht bewertbar“ heißt: sie gilt, aber es gibt keine Anforderungszeilen; ohne Nachweis gilt nichts als erfüllt. Quelle: BSI-Standard 300-1, Kap. 2.2.

Objektart Komponente ☐ nur Lücken

Compliance-Verpflichtung	Komponente Backup-Plattform	Komponente Keycloak IdP	Komponente Leitstellen-Plattform	Komponente MessWerk Digital SMGW-Backend	Komponente MobilStrom Ladeinfrastruktur-Backend	Komponente NordPay Zahlungsreferenzdienst	Komponente Portal-Plattform Nordstern
DSGVO	⚠ Offen 6/20	⚠ Offen 9/30	◌ nicht bewertbar	–	–	✓ Erfüllt 10/10	◌ nicht bewertbar
EnWG/MsbG-Marktkommunikation ⚠ rechtlicher Faktor geändert	–	? Ohne Katalog	–	–	–	? Ohne Katalog	–
BSI-Mindeststandard zur Nutzung von TLS	⚠ Offen 4/16	⚠ Offen 6/24	◌ nicht bewertbar	✓ Erfüllt 8/8	–	–	◌ nicht bewertbar
NIS2-Umsetzungsgesetz	–	⚠ Offen 44/218	–	✓ Erfüllt 97/97	✓ Erfüllt 65/65	–	◌ nicht bewertbar
ISO/IEC 27001:2022 Annex A	✓ Erfüllt 24/24	✓ Erfüllt 36/36	–	✓ Erfüllt 12/12	⚠ Offen 3/12	–	–

- **Erfüllt:** alle anwendbaren Anforderungen umgesetzt.
- **Offen:** mindestens eine fehlt noch.
- **Nicht bewertbar:** die Verpflichtung gilt, aber es gibt noch keine Anforderungen aus dem Katalog.

Was fehlt noch?

Unsere Interpretation · keine Vorgabe des Standards

Vier Arten von Lücken, jeweils mit Zahl und den ersten Fällen. Von dort geht es direkt zur Stelle, an der sie sich schließen lassen. Das Tool sperrt nichts.

Was fehlt noch?

Hinweise auf Lücken. Sie sperren nichts. Quelle: BSI-Standard 300-1, Kap. 2.2.

16 Objekte ohne Compliance-Verpflichtung
Ordnen Sie eine Verpflichtung zu oder halten Sie fest, dass keine gilt.

- Störungsannahme und Kundenkommunikation — Zuordnen
- Notfallmanagement Erdgasnetz — Zuordnen
- Mahnwesen für Ladeinfrastruktur-Kunden — Zuordnen

alle 16 anzeigen

3 Compliance-Verpflichtungen ohne Wirkung
Ordnen Sie der Verpflichtung ein Objekt im Geltungsbereich zu.

- Verfügbarkeitszusage Fernwärme-Großabnehmer — Zuordnen
- Berichtspflicht Informationssicherheit an den Aufsichtsrat — Zuordnen
- Meldung von Sicherheitsvorfällen an den Netzbetreiber binnen 24 Stunden — Zuordnen

9 Dienstleister ohne gültigen Nachweis
Für die vertraglichen Verpflichtungen fehlt ein gültiger, akzeptierter Nachweis. Verknüpfen Sie einen.

- NordPay GmbH — Zuordnen
- Datacenter Süd eG — Zuordnen
- NordTech Systems AG — Zuordnen

alle 9 anzeigen

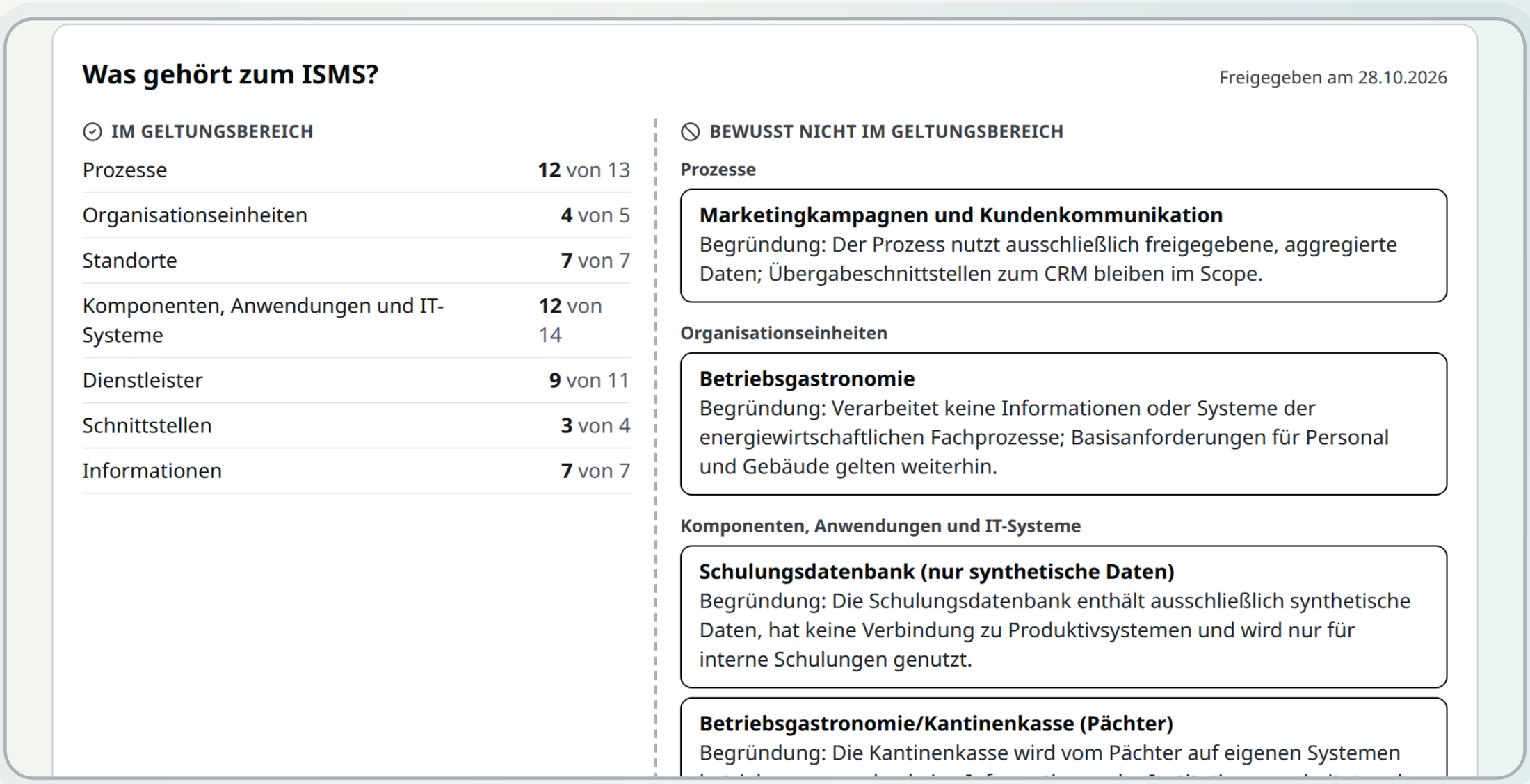
5 Nicht erfüllte Erwartungen ohne Maßnahme
Die Erwartung wurde übernommen, aber keine Maßnahme setzt sie um. Verknüpfen Sie eine.

- Verfügbarkeit des Kundenportals von mindestens 99,5 Prozent — Zuordnen
  von Kundinnen und Kunden (Haushalte und Gewerbe)
- Jährlicher Nachweis der Wirksamkeit der Sicherheitsmaßnahmen — Zuordnen
  von Bundesnetzagentur (Regulierung)

Alles gehört dazu, außer es ist begründet.

BSI-STANDARD 300-1 VERLANGT
Aus Kontext und Compliance-Verpflichtungen legt die Institutionsleitung fest, was zum ISMS gehört: Geschäftsprozesse, Institutionseinheiten, Standorte, Anwendungen, IT-Systeme. Ausgeschlossenes kann benannt werden.

BEI BLUEPROCEEDINGS ISMS
Wir drehen es um: Alles Erfasste gehört dazu, ausgeschlossen wird nur mit Begründung. So fällt kein System versehentlich heraus.



In der Oberfläche heißt der Anwendungsbereich „Geltungsbereich“.

Wer erwartet was?

BSI-STANDARD 300-1 VERLANGT
Interne und externe Stakeholder identifizieren (z. B. Kunden, Aufsicht, Personalvertretung), ihre Erwartungen dokumentieren, Relevanz und Priorität festlegen und mit der Institutionsleitung klären, was verbindlich ins ISMS kommt.

BEI BLUEPROCEEDINGS ISMS
Jede Erwartung hält fest, ob sie übernommen wird und wie weit sie erfüllt ist. Stakeholder bekommen ein Gewicht von 1 bis 5, das freigegeben wird.

Erwartung
übernommen oder nicht, mit Begründung

↓

Gewicht
1 bis 5, freigegeben

↓

Erfüllung
aus den zugeordneten Maßnahmen



Woher wissen wir, was zuerst dran ist?

Unsere Interpretation · keine Vorgabe des Standards

Das Gewicht der Stakeholder fließt in einen Vorschlag für die Reihenfolge der Maßnahmen ein, von P1 bis P5. Es gibt keine Gesamtpunktzahl: Die höchste Einzelklasse bestimmt den Vorschlag, und man sieht, welcher Grund das ist.

Maßnahme: **ISB-Review der neuen RACI-Informationsverbundabdeckung** · Vorschlag P4. Die höchste Einzelklasse bestimmt den Vorschlag.

Faktoren

Überfälligkeiten Frist überschritten Nachweise, Ausnahmen, Maßnahmenplan	P1 P2 P3 **P4** P5 – – – ◇ – ○ Bestimmt die Klasse
Modalverb und Sicherheitsniveau SOLLTE, normal-SdT Katalog	P1 P2 **P3** P4 P5 – – ◇ – – ○ Ohne Wirkung auf die Klasse
Aufwand Stufe 3 Katalog	P1 P2 P3 P4 P5 – – – – – ○ Ohne Wirkung auf die Klasse

Stakeholder-Gewichtung

9 Stakeholder, Summe 35, höchste Gewichtung 5; 1 ausdrücklich nicht übernommen (nicht gezählt)

Geschäftsführung der Stadtwerke	■■■■□ Gewicht 4 von 5
IT-Betrieb und Leitstellentechnik	■■■■□ Gewicht 4 von 5
Übertragungs- und Verteilnetzbetreiber (Netzkopplung)	■■■■□ Gewicht 4 von 5
+ 6 weitere Stakeholder, siehe Detailansicht der Maßnahme	
Ergebnis der Stakeholder-Gewichtung	P1 P2 P3 **P4** P5 – – – ◇ – ○ Gleichauf

Hier bestimmt die überschrittene Frist die Klasse P4. Eine manuell gesetzte Priorität bleibt sichtbar.

Prozesse und Schutzbedarf.

BSI-STANDARD 300-1 VERLANGT

Die Geschäftsprozesse im Anwendungsbereich dokumentieren (2.5) und je Prozess den Schutzbedarf für Vertraulichkeit, Integrität und Verfügbarkeit feststellen: normal oder hoch (2.6). Bei hoch ist eine Risikobetrachtung nötig.

BEI BLUEPROCEEDINGS ISMS

Jeder Prozess zeigt seinen Schutzbedarf je Schutzziel und die verantwortliche Rolle. Oben steht, wo noch Angaben fehlen.

Welche Prozesse tragen die Institution, und wo fehlen Angaben?

0
Prozesse mit offenen Angaben
Owner, Schutzbedarf und Informationsverbund sind überall gepflegt

7
Hauptprozesse und eigenständige Prozesse

6
Teilprozesse

Energiedienstleistungen: Netzbetrieb und Kundenversorgung
Hauptprozess
Bündelt als Sammelprozess die operative Verantwortung von der Netzsteuerung bis zur Kundenabrechnung auf Ebene der Geschäftsführung.
Verantwortlich: Institutionsleitung / Geschäftsführung
C **normal** · I **hoch** · A **hoch** · AUTH **normal**

Kundenabrechnung und Marktkommunikation
Hauptprozess
Erstellt Rechnungen für Strom- und Gaskunden, verarbeitet Zahlungseingänge und tauscht Wechsel- und Marktdaten mit anderen Marktpartnern aus.
Verantwortlich: Fachverantwortliche
C **normal** · I **hoch** · A **hoch** · AUTH **normal** · TRACE **normal**

C, I, A: Vertraulichkeit, Integrität, Verfügbarkeit. AUTH (Authentizität) und TRACE (Nachvollziehbarkeit) hat die Demo-Institution als eigene Schutzziele ergänzt.

15 2.7 · 2.8 · 2.9

Leitlinie, Rollen, Dokumentation.

BSI-STANDARD 300-1 VERLANGT

Eine Leitlinie mit Zielen und Strategie, freigegeben und allen kommuniziert (2.7). Rollen und Zuständigkeiten ohne Interessenskonflikte (2.8). Verfahren für Kommunikation und Dokumentenlenkung (2.9).

BEI BLUEPROCEEDINGS ISMS

Die Leitlinie hat Fassungen mit Freigabe und Termin zur Überprüfung und entsteht als PDF aus dem freigegebenen Stand. Die RACI-Matrix legt je Tätigkeit fest, wer durchführt und wer rechenschaftspflichtig ist.



Freigegeben, mit Termin.

BSI-STANDARD 300-1 VERLANGT

Die Institutionsleitung trägt die Verantwortung und gibt frei, u. a. Anwendungsbereich, Schutzbedarf, Ressourcen und Leitlinie (2.10). Sie autorisiert den Rahmen für die Risikobetrachtung: strategisch, methodisch, organisatorisch (2.11).

BEI BLUEPROCEEDINGS ISMS

Jede Freigabe hat eine Fassung, eine freigebende Rolle, ein Datum und einen Termin zur Überprüfung. Der Risikorahmen zeigt die drei Ebenen des Standards und was noch fehlt.

Schutzbedarf (Methodik) — Freigegeben

Fassung Version 2	Freigegeben am 01.11.2026
Freigegeben von Institutionsleitung / Geschäftsführung	Gültig ab 27.10.2026

Nächste Überprüfung: 27.10.2027

- Fassung
- freigegeben von (Rolle)
- gültig ab
- nächste Überprüfung

Steht der Rahmen für die Risikobetrachtung? — BSI-Standard 300-1, Kap. 2.11

Strategisch
Wie viel Risiko tragen wir?

- Risikoappetit festgelegt (Matrix Version 3)
- Risikoakzeptanzkriterien als Regeln der Matrix
- Die Institutionsleitung entscheidet nur über Restrisiken oberhalb des Risikoappetits

Methodisch
Wie bewerten wir Risiken?

- Verfahren für Risikoidentifikation, -bewertung und -behandlung beschrieben · Rahmenwerk
- Kriterien der Risikobewertung in Matrix Version 3

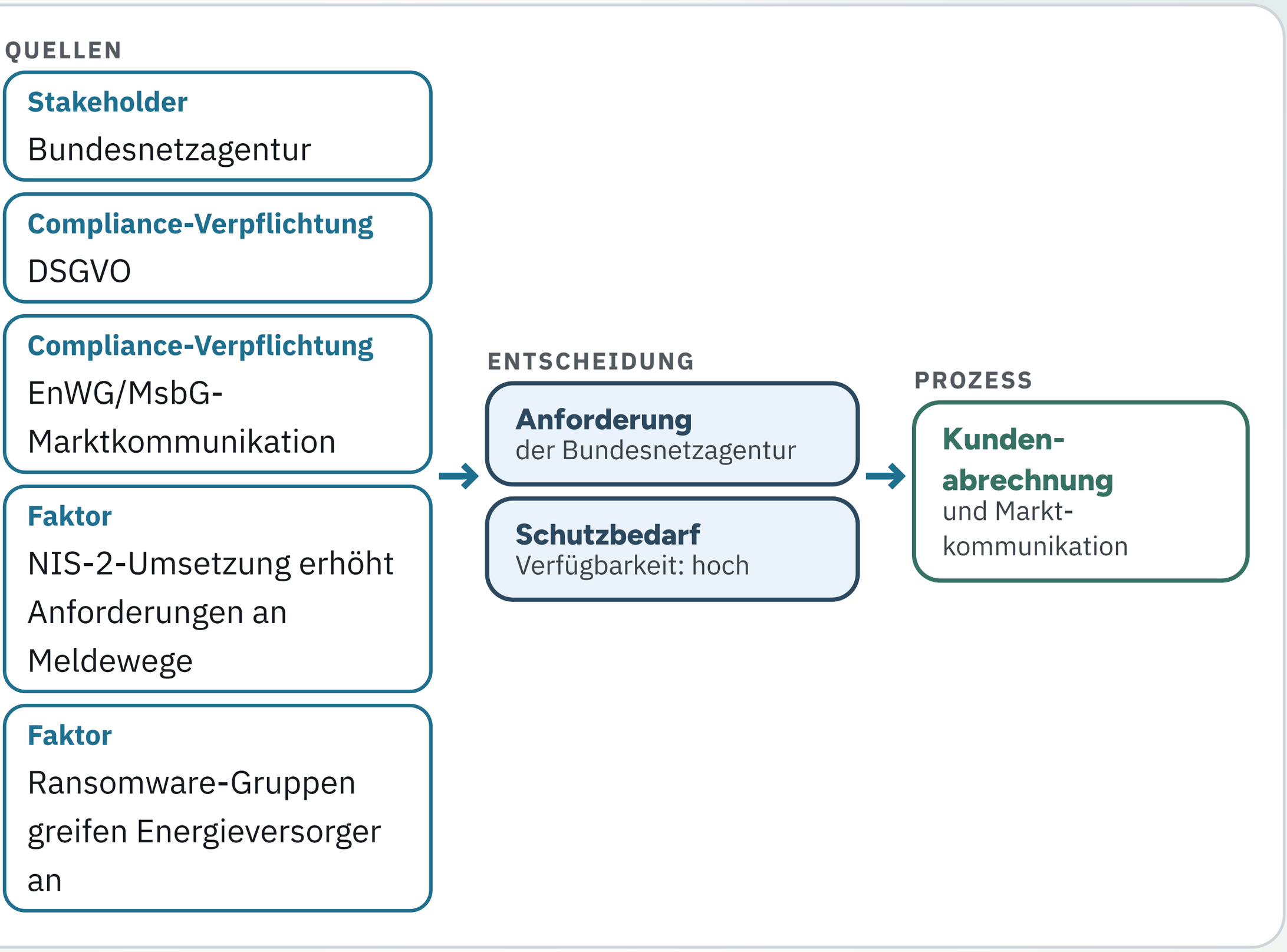
Organisatorisch
Wer trägt welches Risiko?

- Risikoeigentümer: 14 Risiken zugewiesen
- ⚠ 5 Risiken ohne Risikoeigentümer · Risiken

Warum tun wir das?

Unsere Interpretation · keine Vorgabe des Standards

Zu einem Prozess zeigt das ISMS-Tool, welche Stakeholder, Compliance-Verpflichtungen und Faktoren zu welchen Entscheidungen geführt haben. Nachgezeichnet aus der Demo:



Vereinfacht nachgezeichnet. Ein Faktor, eine Compliance-Verpflichtung oder eine Erwartung, die sich ändert, führt so direkt zu den Entscheidungen, die neu zu prüfen sind.

18 WIE GEHT ES WEITER?

Als Nächstes: das Wie.

NÄCHSTER BEITRAG

How-To: Prozessschritt 1 – Erhebung und Planung

Von der leeren Instanz bis zum abgeschlossenen Prozessschritt 1: in welcher Reihenfolge und wo das ISMS-Tool hilft, es besser zu machen.

11.11., 17 Uhr: Vorstellung per Videokonferenz

Live-Vorstellung des ISMS-Tools, wenn genug Interesse besteht. Wer dabei sein will, schreibt eine Nachricht, der Link folgt. Am selben Tag startet die Testphase für bis zu elf Personen aus der ISMS-Praxis.

Die Reihe entsteht ohne Werbebudget. Wenn sie euch weiterhilft:

1. **Teilen** mit allen, die gerade an Grundschutz++ arbeiten
2. **Folgen** der Seite von BlueProceedings, dort geht es weiter

Mich interessiert:

Wo haltet ihr heute fest, warum eine Entscheidung so getroffen wurde? Ich freue mich über Erfahrungen und Widerspruch.

Testphase	blueproceedings.de/#download
Methodik in fünf Schritten	blueproceedings.de/bsi-standard-300-1
Neuigkeiten	linkedin.com/company/blueproceedings