



Pre-Alpha · Grundschutz++

Grün – oder nur unwidersprochen?

Ein erster Blick in ein ISMS, das mitläuft, statt nach der Freigabe zu veralten. In elf Folien.

Wischen für den Einblick →



Eine Tabelle hält nur fest.

Sie zeigt eine Momentaufnahme. Mit der Freigabe ist ein ISMS nicht fertig.

Aktualität

Dass ein Konzept nach Monaten veraltet ist, wissen die meisten. Neue Vorgaben, Systeme und Dienstleister überholen es schnell.

Verantwortung

Sie steht im Organigramm, doch im Alltag bleibt offen, wer entscheidet und wer einspringt, wenn jemand fehlt.

Prüfung

Aus „erledigt“ wird schnell „wirksam“, ohne dass es jemand geprüft hat.

Verbesserung

Abweichungen und Risiken werden notiert, doch es bleibt unklar, was sie für Prozesse und Systeme bedeuten.

Alles hängt zusammen.

Jedes Glied kennt seine Herkunft. Ändert sich eines, wird sichtbar, was neu bewertet werden muss.

1

Prozesse und Informationen

Was die Institution tut und braucht

2

Komponenten und Dienstleister

Worauf es läuft, mit Abhängigkeiten

3

Schutzbedarf

Je Schutzziel, mit Begründung

4

Anforderungen

Aus dem Katalog, je Objekt, mit Herkunft

5

Risiken

Bewertet, behandelt, akzeptiert mit Wiedervorlage

6

Maßnahmen

Mit Verantwortung, Frist und Meilensteinen

7

Nachweise

Geprüft, versioniert, mit Ablaufdatum

8

Wirksamkeit

Gegen Kriterien geprüft, nicht nur abgehakt

9

Freigabe

Mit vier Augen, Person, Rolle, Zeitpunkt

Veraltet statt falsch-grün.

Ändert sich nach der Freigabe eine Grundlage, wird das Sicherheitskonzept als veraltet markiert. Mit Ursache, Zeitpunkt und Rolle.

Kunden- und Marktpartnerportal (KMP)

Status: aktiv · Sicherheitsniveau: erhöht · Quelle: Blaupause Versorgungsportal mit externem Zugriff · Kritikalität: hoch

Kunden- und Marktpartnerportal (KMP): fachlicher End-to-End-Prozess mit dokumentierten Schnittstellen und Verantwortlichkeiten.

- ✓ Je Ursache: wann zuletzt geändert, wie oft, von wem
- ✓ Der Bericht lässt sich mit einem Klick neu erzeugen

Wirkung zeigen.

Bei einem Vorfall schlägt die Ausbreitungsprüfung vor, was über Abhängigkeiten mitbetroffen sein könnte. **Erreichbar heißt nicht betroffen:** Du bestätigst, verwirfst oder lässt offen, jeweils mit Begründung.

Ausbreitungsprüfung

Die Prüfung schlägt vor, welche weiteren Objekte betroffen sein könnten – über Abhängigkeiten und bestätigte Schnittstellen. Ein erreichbares Objekt gilt nicht automatisch als betroffen: Erst Ihre Bestätigung mit einer Aussage zur Wirkung je Schutzziel dokumentiert sie.

15 Objekte erreichbar

3 bestätigt

8 zu prüfen

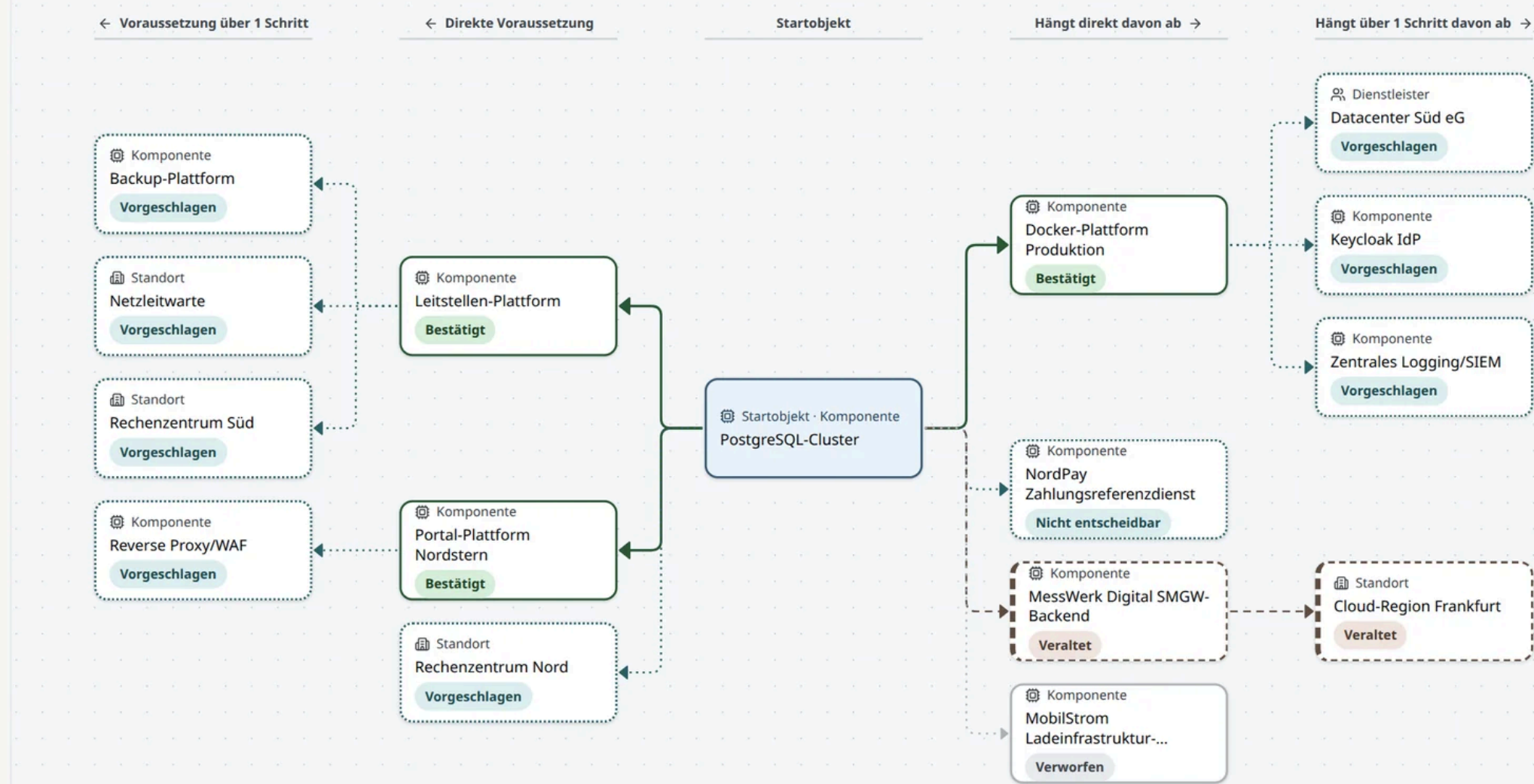
2 anders entschieden

2 veraltet

Richtung: Beide Richtungen · Prüfung läuft

Graph

Liste



☐ Bestätigt: Wirkung dokumentiert ☐ Vorgeschlagen: noch zu prüfen ☐ Veraltet: Beziehung geändert ☐ Verworfen mit Begründung

Pfeile zeigen, wohin sich ein Vorfall am Startobjekt auswirken kann. Je Objekt ist der kürzeste Weg gezeichnet; 9 weitere Verbindungen stehen beim gewählten Objekt und in der Liste.

Erledigt ist nicht wirksam.

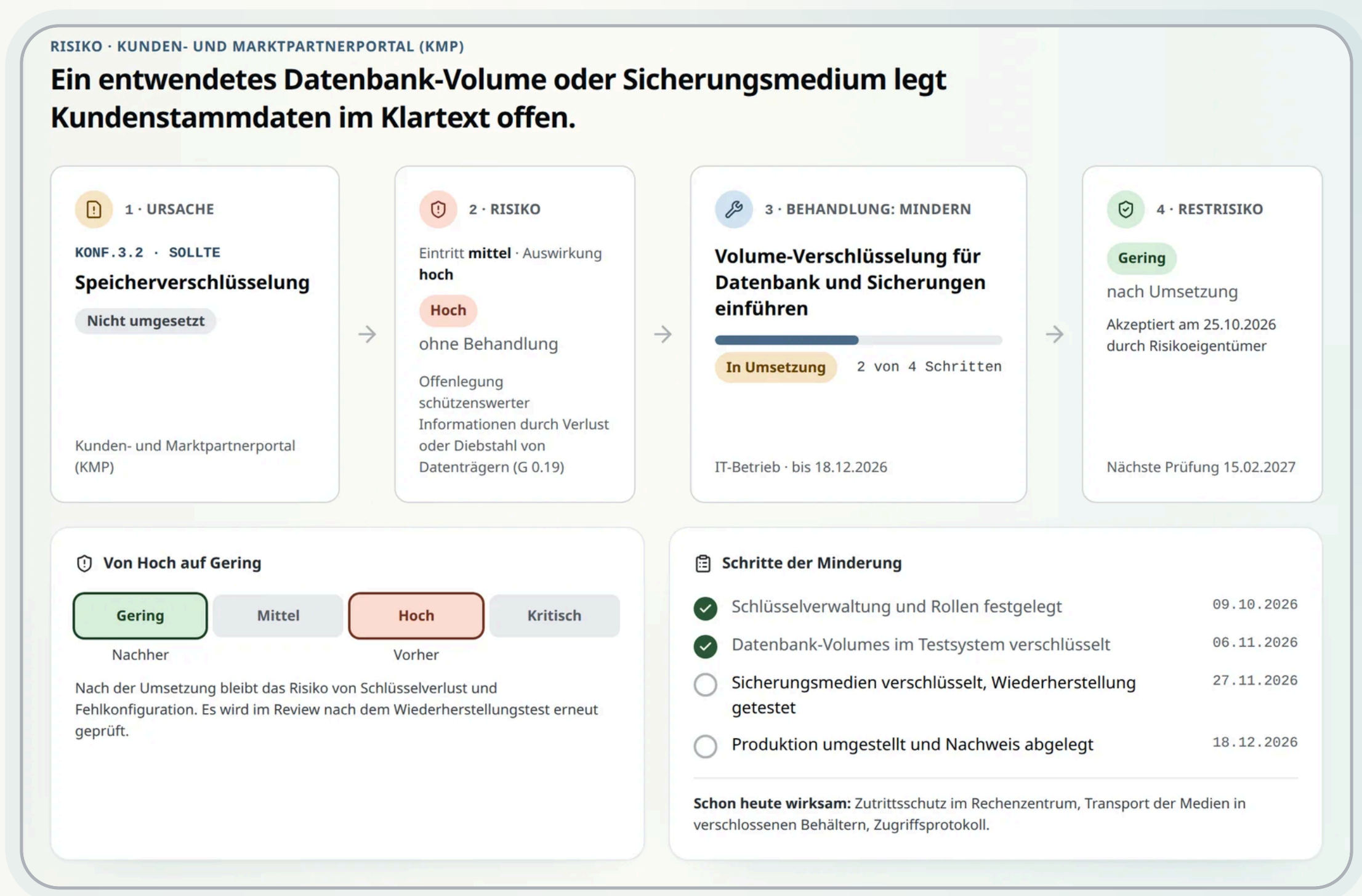
Eine Maßnahme schließt erst, wenn vorab festgelegte Kriterien geprüft sind und ein gültiger Nachweis vorliegt. Bis dahin bleibt der Abschluss gesperrt und sagt, was fehlt.



- ✓ Messbare Kriterien, bevor geprüft wird
- ✓ Nur akzeptierte, gültige Nachweise schließen ab
- ✓ Die Schließung gibt eine zweite Person frei

Von der Ursache zum Restrisiko.

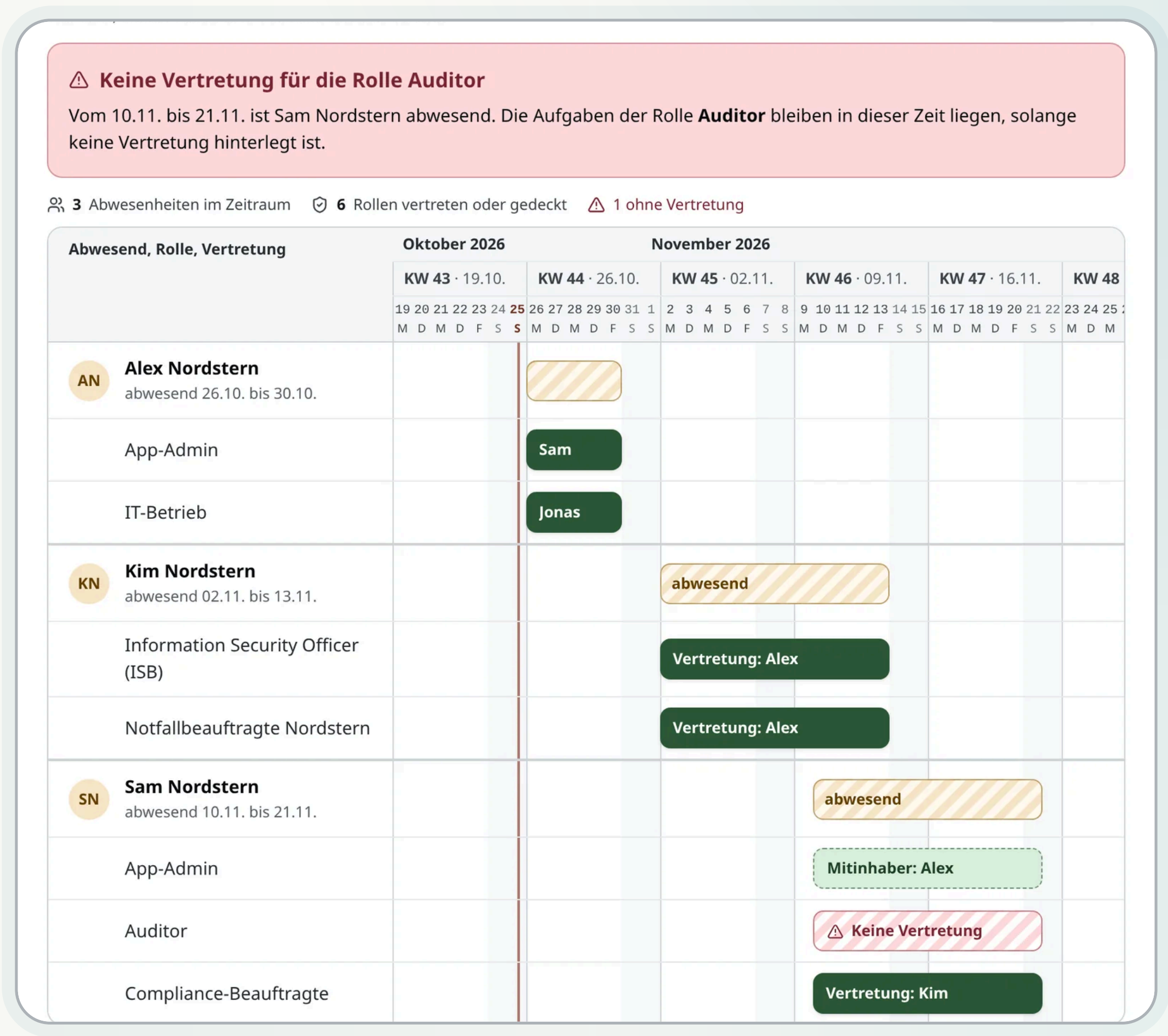
Jedes Risiko hat eine Seite: woher es kommt, wie es behandelt wird und was danach übrig bleibt. Die Maßnahme steht als Verweis daneben.



- ✓ Ursache ist hier eine noch nicht umgesetzte Anforderung
- ✓ Restrisiko braucht die Akzeptanz des Risikoeigentümers

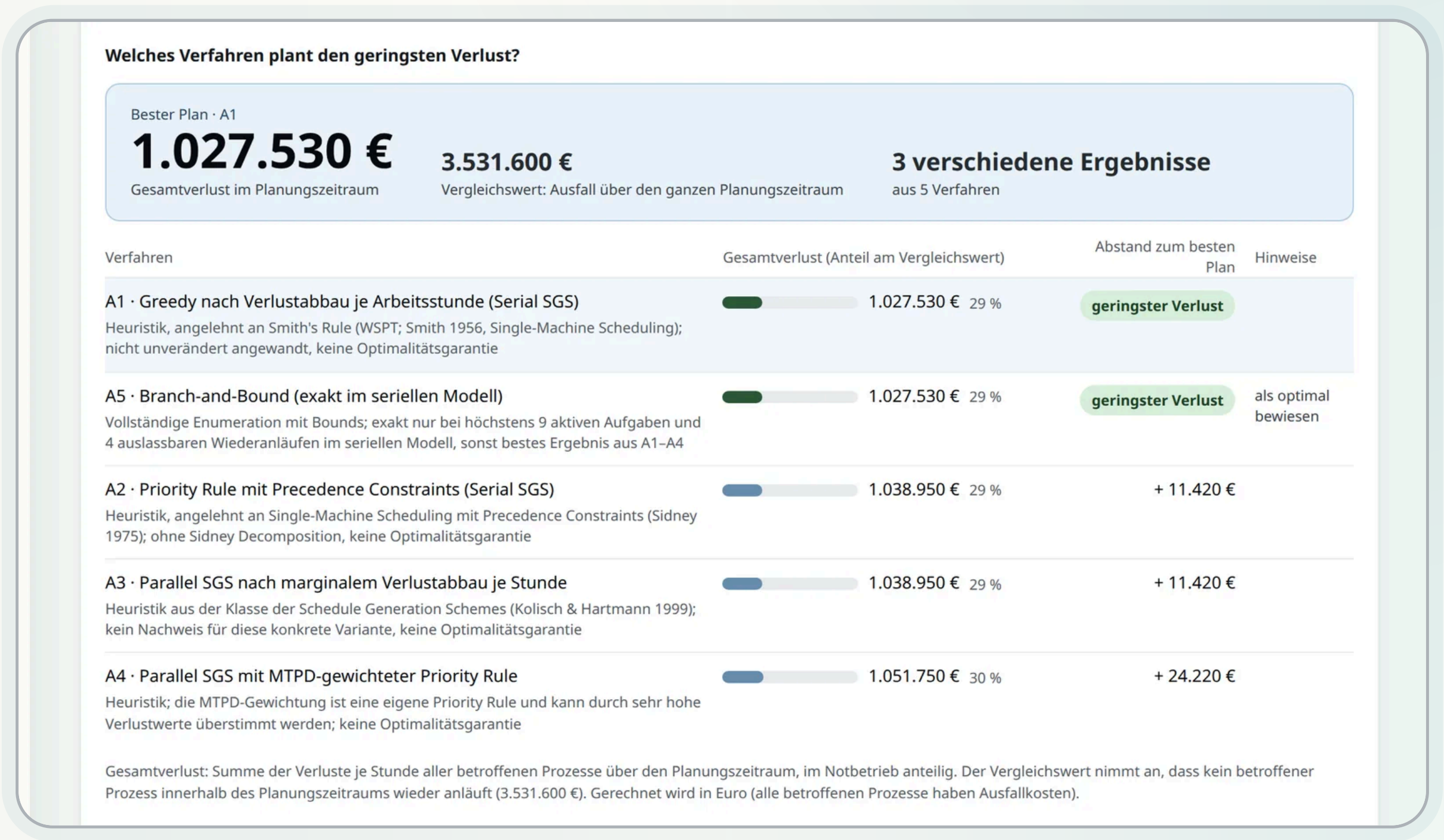
The ISMS must go on.

Der Vertretungsplan zeigt, wer fehlt, wer vertritt und wo niemand einspringt, bevor eine Rolle unbesetzt ist.



Wiederaanlauf planen, bevor es ernst wird.

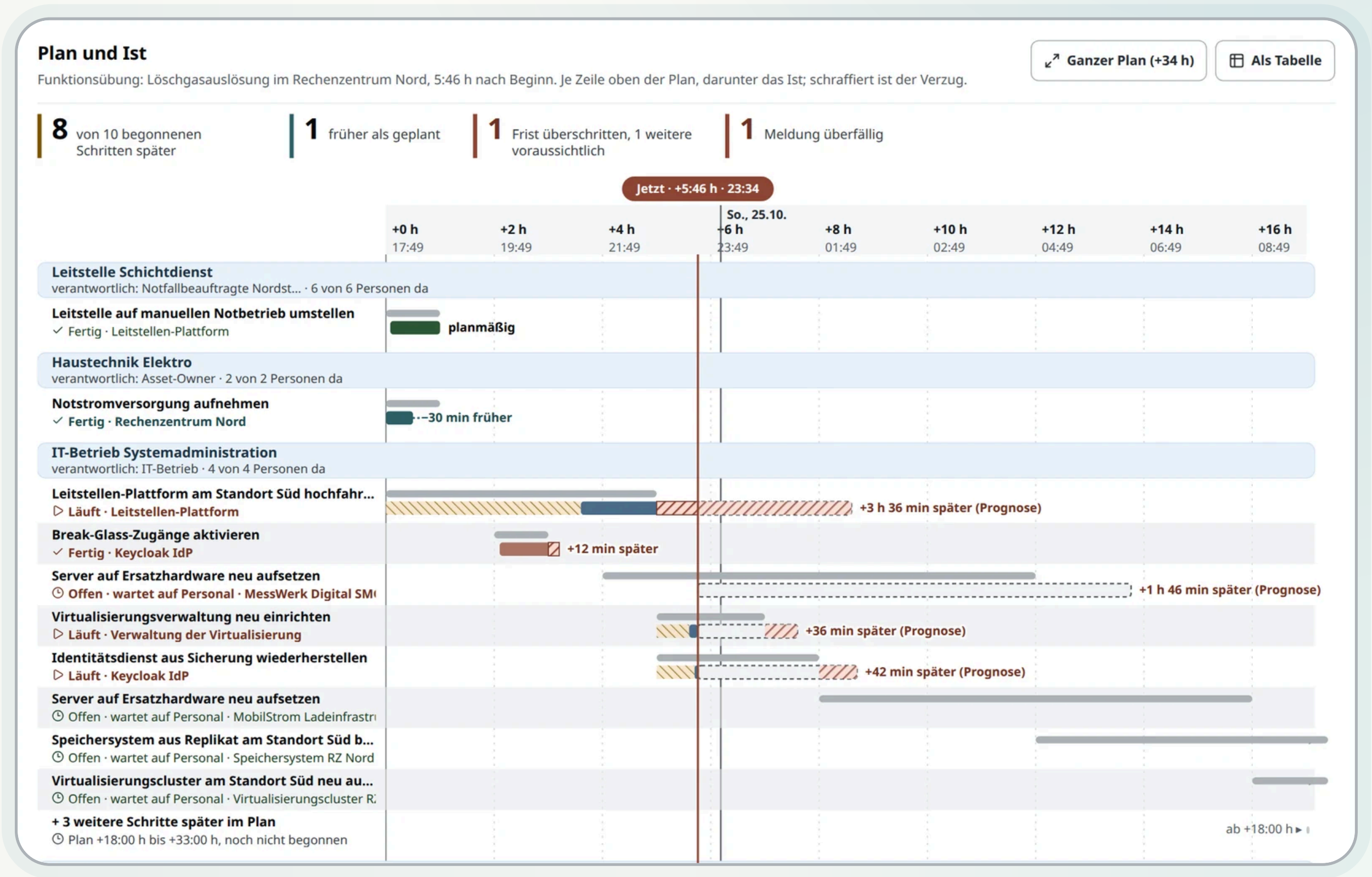
Fünf Planungsverfahren im Vergleich, bewertet am modellierten Verlust. Ein Planungsvorschlag, keine Entscheidung: Der Krisenstab entscheidet selbst.



- ✓ Reihenfolge und Zeiten je Notfallprozess
- ✓ Als Übung oder echter Krisenlauf speicherbar

Ein Plan ohne Übung sagt wenig.

Im Lagezentrum steht der Plan einer Übung neben dem, was im Durchlauf geschieht. Schraffiert ist der Verzug.



Der Plan.

27.10.2026 ○ **BSI stellt Grundschutz++ vor**
auf der it-sa in Nürnberg

ab 11.11.2026 ○ **Testphase**
Bis zu elf Personen aus der ISMS-Praxis testen die Pre-Alpha. Deshalb elf Folien.

01.01.2027 ○ **Grundschutz++ zertifizierbar**
laut BSI

Januar 2027 ● **Erste Version (geplant)**
Docker auf eigener Infrastruktur, ohne Hersteller-Cloud

Kennst du jemanden, der Grundschutz++ einführt?

Schick ihm oder ihr diesen Beitrag weiter. Und was fehlt dir im ISMS? Schreib es in die Kommentare.

