



Schritt 1: Erhebung und Planung.

Elf Teilschritte, ein Ort. Und eine Arbeitsteilung, die Leitung und ISB entlastet.

1
Erhebung
und Planung

2
Anforderungs-
analyse

3
Realisierung

4
Überwachung

5
Kontinuier-
liche
Verbesserung



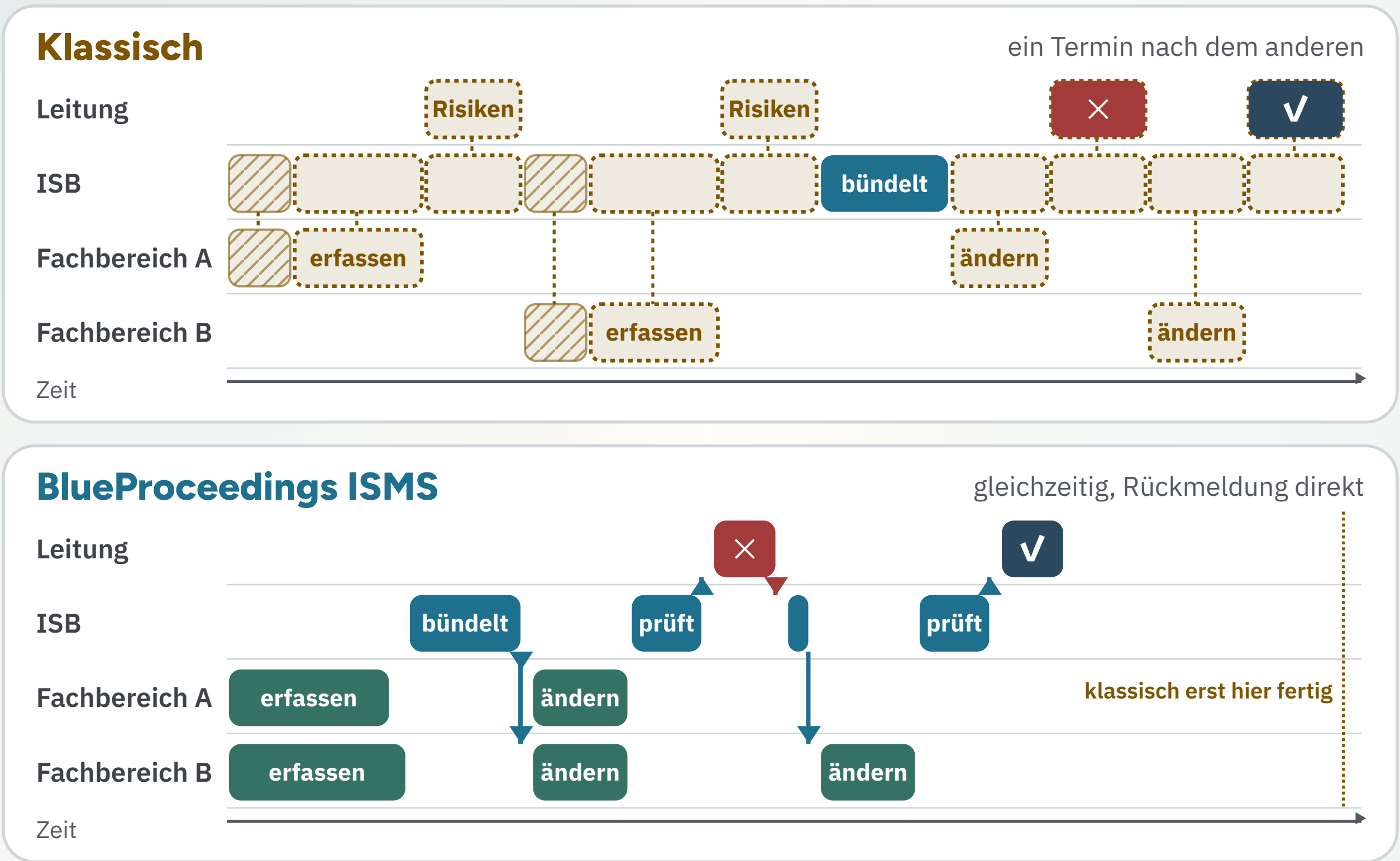
Elf Teilschritte, ein Ort.

Der BSI-Standard 300-1 beschreibt Schritt 1 in Kap. 2.1 bis 2.11. So bildet BlueProceedings ISMS jeden davon ab.

2.1	Kontext der Institution Interne und externe Einflussfaktoren, mit Entscheidungen verknüpft	✓
2.2	Compliance-Management Gesetze, Verträge und eigene Pflichten in einem Register	✓
2.3	Anwendungsbereich Alles gehört dazu, Ausschluss nur mit Begründung	✓
2.4	Interessierte Parteien Stakeholder mit Anforderungen und Gewichtung	✓
2.5	Geschäftsprozesse Abhängigkeiten, RTO und RPO, Wiederanlauf	✓
2.6	Schutzbedarf Normal oder hoch je Grundwert, mit Kriterien	✓
2.7	Leitlinie Versioniert, freigegeben, kommuniziert	✓
2.8	Rollen und Zuständigkeiten RACI-Matrix, Vertretung, Funktionstrennung	✓
2.9	Dokumentation und Kommunikation ISMS-Dokumente mit Freigaben	✓
2.10	Freigabe der Vorgehensweise Freigaben mit Person, Rolle und Zeitpunkt	✓
2.11	Risikobetrachtung Risikomatrix mit Risikoappetit und Zellregeln	✓

Nacheinander oder parallel.

Klassisch holt der ISB jeden Fachbereich in einen Termin und trägt jedes Ergebnis zur Leitung. In BlueProceedings ISMS erfassen die Fachbereiche gleichzeitig selbst.



Verteilen, ohne zu verwässern.

Wer einen Prozess oder ein System verantwortet, macht die Angaben selbst. Der ISB steuert, die Leitung gibt frei. Die RACI-Matrix hält fest, wer was tut.

Institution

TÄTIGKEIT	R	A	C	I
ISMS-Leitlinie	Informationssicherheitsbeauftragte (ISB) ×	Institutionsleitung / Geschäftsführung	Fachverantwortliche × Asset-Owner ×	Auditor ×
Geltungsbereich	Informationssicherheitsbeauftragte (ISB) ×	Institutionsleitung / Geschäftsführung	Fachverantwortliche × Asset-Owner ×	Auditor ×
Register	Fachverantwortliche ×	Institutionsleitung / Geschäftsführung	Informationssicherheitsbeauftragte (ISB) × Asset-Owner ×	Auditor ×
Risikomanagement und Ausnahmen	Informationssicherheitsbeauftragte (ISB) ×	Institutionsleitung / Geschäftsführung	Fachverantwortliche × Risikoeigentümer ×	Auditor ×

Informationsverbund Netzleitstelle: zwei C, mehrere I

TÄTIGKEIT	R	A	C	I
Schutzbedarf dieses Informationsverbunds	Fachverantwortliche ×	Institutionsleitung / Geschäftsführung	Informationssicherheitsbeauftragte (ISB) × Compliance-Beauftragte ×	Auditor × IT-Betrieb × Notfallbeauftragte Nordstern ×
Risikomanagement dieses Informationsverbunds	Fachverantwortliche ×	Institutionsleitung / Geschäftsführung	Informationssicherheitsbeauftragte (ISB) × Compliance-Beauftragte ×	Auditor × Notfallbeauftragte Nordstern ×
Umsetzung dieses Informationsverbunds	Technisch-Verantwortlicher ×	Fachverantwortliche	Informationssicherheitsbeauftragte (ISB) × IT-Betrieb ×	Auditor × Notfallbeauftragte Nordstern ×

R **Responsible**
führt aus, z. B. erfasst den Prozess

A **Accountable**
genau eine Rolle, entscheidet und gibt frei

C **Consulted**
wird vorher gefragt, auch mehrere

I **Informed**
erfährt das Ergebnis, auch mehrere

- ✓ Getrennt davon: Vertretungsplan, wer einspringt
- ✓ Keine Begrenzung der Nutzerzahl

Wenn sich ein Faktor ändert.

Interne und externe Einflussfaktoren lassen sich mit Entscheidungen verknüpfen. Ändert sich einer, zeigt seine Seite, welche Freigaben, Risikobewertungen, Schutzbedarfe und Maßnahmen neu zu prüfen sind.

EINFLUSSFAKTOR FAK-001

NIS2-Umsetzung und KRITIS-nahe Nachweispflichten erhöhen die Anforderungen an Governance, Meldewege und Lieferkettensicherheit.

Externer Faktor · wirksam in Version 3 · Eigentümerrolle: Informationssicherheitsbeauftragte (ISB)

Ein Faktor ist eine Entscheidungsgrundlage. Er erzeugt keine Risiken, Maßnahmen oder Aufgaben und sperrt keine Freigabe.

Wirksamer Stand

Quelle
EU 2022/2555; nationaler Umsetzungsstand 2026; Rechtskataster LEG-CYB-02

Annahmen
Die Stadtwerke fallen ab 2027 in den erweiterten Anwendungsbereich. Nach der Konkretisierung der Meldepflichten gilt für erhebliche Sicherheitsvorfälle eine Meldefrist von 24 Stunden.

Gültig ab / bis
2026-10-28 / 2028-10-27

Sicherheitsrelevanz
hoch

Unsicherheit
Stand 28.10.2026: Die Detailfristen des nationalen Umsetzungsgesetzes sind noch nicht endgültig; der Anwendungsbereich wird zum Review im April 2027 erneut geprüft.

Nächster Review
2027-04-28

Auswirkung einer Ablösung oder Rücknahme

10 Entscheidungen nennen diesen Faktor in 2 Informationsverbund/-verbünden, 8 davon ohne Verbundbezug. Bei einer *materiellen* Nachfolgeversion oder einer Rücknahme erhält jede dieser Entscheidungen einen Prüfhinweis; 6 davon beziehen sich auf eine dokumentierte Aktion und brauchen zur Bestätigung die zuständige Freigabekompetenz. Redaktionelle Änderungen erzeugen keinen Hinweis. Die Hinweise blockieren weder Einreichung noch Freigabe noch Ausgabe.

Prüfhinweise zur Entscheidungsgrundlage

Offen

Risiko: Für die Störungsannahme der Leitstelle außerhalb der Dienstzeiten gibt es nur einen Dienstleister ohne Ausweichmöglichkeit. · neue materielle Version 3 · 2026-10-28

Zur Entscheidung

Offen

ISMS-Dokument: Meldeweg NIS2 für erhebliche Sicherheitsvorfälle (Version 1) · neue materielle Version 3 · 2026-10-28

Zur Entscheidung

Offen

Schutzbedarfsfeststellung: Kunden- und Marktpartnerportal (KMP) · Verfügbarkeit: hoch · neue materielle Version 3 · 2026-10-28

Zur Entscheidung

Offen

Maßnahme: Redundante SIEM-Anbindung der Süd-Leitstelle · neue materielle Version 3 · 2026-10-28

Zur Entscheidung

Offen

Schutzbedarfsfeststellung: Notfallmanagement Erdgasnetz · Verfügbarkeit: hoch · neue materielle Version 2 · 2026-10-28

Zur Entscheidung

Ausschnitt vergrößert

Prüfhinweise zur Entscheidungsgrundlage

- Offen

Risiko: Für die Störungsannahme der Leitstelle außerhalb der Dienstzeiten gibt es nur einen Dienstleister ohne Ausweichmöglichkeit. · neue materielle Version 3 · 2026-10-28

Zur Entscheidung
- Offen

ISMS-Dokument: Meldeweg NIS2 für erhebliche Sicherheitsvorfälle (Version 1) · neue materielle Version 3 · 2026-10-28

Zur Entscheidung
- Offen

Schutzbedarfsfeststellung: Kunden- und Marktpartnerportal (KMP) · Verfügbarkeit: hoch · neue materielle Version 3 · 2026-10-28

Zur Entscheidung
- Offen

Maßnahme: Redundante SIEM-Anbindung der Süd-Leitstelle · neue materielle Version 3 · 2026-10-28

Zur Entscheidung



Pflichten an einem Ort.

Gesetze, Verträge und Satzungen als Ursprung der Anforderungen, jede Pflicht mit ihrem eigenen Katalog, ihrer Kritikalität und ihrer Quelle. Eigene Pflichten direkt in der Oberfläche.

TYP	BEZEICHNUNG	KATALOG	ERFÜLLUNGSSTAND	KRITIKALITÄT	QUELLE
Gesetz	DSGVO	Datenschutz-Anforderungskatalog (DSGVO)	Noch nicht bewertet	Hoch Risikorelevant	VO (EU) 2016/679
Technischer Mindeststandard	BSI-Mindeststandard zur Nutzung von TLS	BSI-Mindeststandard zur Nutzung von TLS	Noch nicht bewertet	Mittel	BSI Entwurf Mindeststandard Bund TLS, Demo-Import 2026
Regulierung	NIS2-Umsetzungsgesetz	Anwenderkatalog Grundschutz++	372 / 998 erfüllt	Hoch Risikorelevant	EU 2022/2555, nationales Umsetzungsgesetz
Norm	ISO/IEC 27001:2022 Annex A	ISO/IEC 27001:2022 Annex A (nur Kennungen und Titel)	Noch nicht bewertet	Mittel	ISO/IEC 27001:2022

Alles gehört dazu, außer es ist begründet.

Jedes erfasste Objekt liegt standardmäßig im Geltungsbereich. Wer etwas herausnimmt, begründet es. Das vermeidet Schatten-IT, weil nichts aus Versehen herausfällt. Für die Übersicht lässt sich die Liste filtern.

Referenzierte Objekte

Alle referenzierbaren Objekte gehören standardmäßig zum Geltungsbereich. Zur Skalierung filtern Sie die Liste; eine Entfernung ist nur als begründeter Ausschluss möglich.

Alle Objektarten

Objekte filtern ...

Im Geltungsbereich (48)

OBJEKTART	OBJEKT	IM GELTUNGSBEREICH	BEGRÜNDUNG (BEI AUSSCHLUSS)
Komponente	PostgreSQL-Cluster	Ja	Nicht erforderlich
Komponente	Docker-Plattform Produktion	Ja	Nicht erforderlich
Information	Kunden- und Vertragsdaten	Ja	Nicht erforderlich
Informationsverbund	Kunden- und Marktpartnerportal (KMP)	Ja	Nicht erforderlich

Ausgeschlossen (2)

OBJEKTART	OBJEKT	IM GELTUNGSBEREICH	BEGRÜNDUNG (BEI AUSSCHLUSS)
Komponente	Schulungsdatenbank (nur synthetische Daten)	Nein	Die Schulungsdatenbank enthält ausschließlich synthetische Daten, hat keine Verbindung zu Produktivsystemen und wird nur für interne Schulungen genutzt. Ausgeschlossen am 28.10.2026, 10:15
Komponente	Betriebsgastronomie/Kantinenkasse (Pächter)	Nein	Die Kantinenkasse wird vom Pächter auf eigenen Systemen betrieben; es werden keine Informationen der Institution verarbeitet und keine Verbindung zum Netz der Institution genutzt. Ausgeschlossen am 28.10.2026, 11:40

Wer was erwartet.

Stakeholder mit ihren Erwartungen. Gewichtet von 1 bis 5 werden ein ganzer Katalog, eine einzelne Anforderung, eine Maßnahme oder eine KPI. Die Gewichtung fließt in die Priorisierung ein.

Gewichtung je Stakeholder

Verknüpfte Anforderungen (strukturiert) ⓘ

Konkrete Kataloganforderungen oder ganze Kataloge, die dieser Stakeholder fordert — gewichtet (1-5) für den Erfüllungsgrad-KPI unten. Erscheint gegenläufig im Anforderungsdetail als „Von Stakeholdern gefordert“.

Ganzer Katalog: Anwenderkatalog Grundschutz++ · Stand 03.07.2026

Gewichtung 4

ARCH.1.1 — Verfahren und Regelungen

Gewichtung 4

Anforderungs-KPI: Umsetzungsquote der Anforderungen

Gewichtung 4

BES.5.13 — Bereitstellung von Datensicherungen

Gewichtung 5

Verknüpfte Maßnahmen ⓘ

Maßnahmen, die dieser Stakeholder für besonders wichtig hält — gewichtet (1-5) für die Wichtigkeits-Statistik unten.

Automatisierte Inventarprüfung der Hardware-Token für privilegierte KMP-Zugänge einführen.

Gewichtung 4

Redundante SIEM-Anbindung der Süd-Leitstelle

Gewichtung 4

Ergebnis: Rangfolge

Wichtigkeits-Statistik: Anforderungen ⓘ	
BES.5.13 — Bereitstellung von Datensicherungen	Ø 4,4 · 5 Stakeholder
SENS.2.8 — Melden von Ereignissen	Ø 4,3 · 3 Stakeholder
TEST.4.4 — Geregelte Notfalländerungen	Ø 4,0 · 5 Stakeholder
ASST.4.4 — Nachweis des Zugangs	Ø 4,0 · 4 Stakeholder
PERS.4.2 — Rollenspezifische Schulungen und Sensibilisierungen	Ø 3,7 · 3 Stakeholder

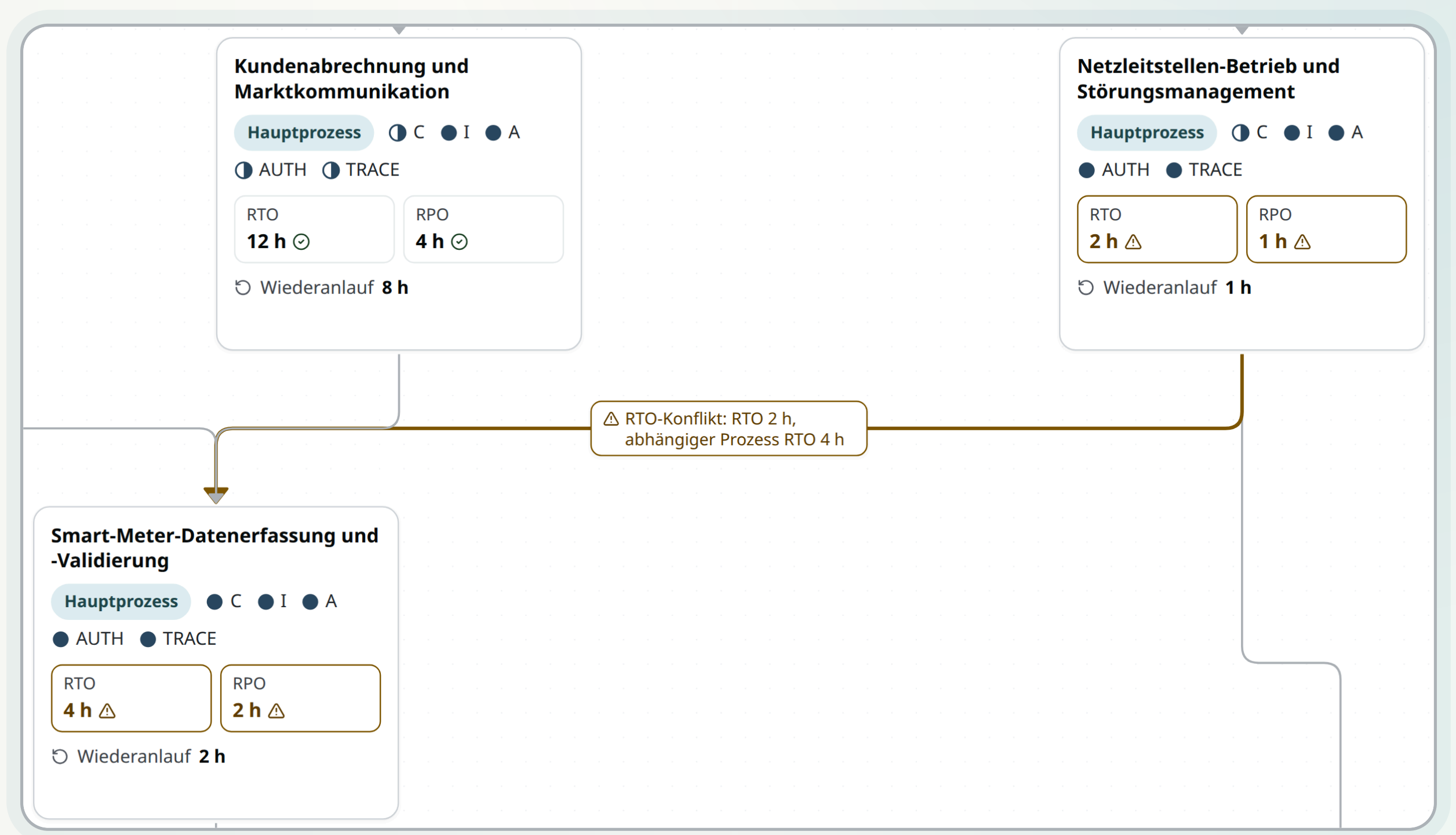
Wichtigkeits-Statistik: Maßnahmen ⓘ	
Redundante SIEM-Anbindung der Süd-Leitstelle	Ø 4,4 · 5 Stakeholder
Nachweisabdeckung für die Netzleitstelle durch zusätzliche automatisierte Prüfläufe erhöhen.	Ø 4,0 · 3 Stakeholder
Zusätzliche Standortredundanz für die Netzleitstelle evaluieren	Ø 4,0 · 2 Stakeholder
Phishing-resistente MFA für KMP-Administration einführen	Ø 4,0 · 1 Stakeholder
Zweiten unabhängigen Zahlungsreferenzdienst evaluieren, um die Abhängigkeit von NordPay zu reduzieren.	Ø 4,0 · 1 Stakeholder

 BlueProceedings ISMS für Grundschutz++ · Pre-Alpha, Demodaten

8 / 15

Wer wen braucht.

Prozesse mit Abhängigkeiten, Schutzbedarf, RTO und RPO. Passen die Zeitvorgaben nicht zusammen, steht der Konflikt am Pfeil.



- ✓ Die Netzleitstelle soll nach 2 h wieder laufen, braucht aber die Smart-Meter-Erfassung, deren RTO 4 h beträgt
- ✓ Das fällt beim Erfassen auf, nicht erst in der Übung

Normal oder hoch, mit Begründung.

Zwei Kategorien je Schutzziel, festgelegt über Schadensszenarien und Regeln für Eskalation und Deeskalation. Schon ein hohes Schutzziel löst die eigene Risikobetrachtung aus.

SCHADENSSZENARIEN (VORLAGEN)				
Szenarien können sich auf die Institution, einen Informationsverbund, jede Zielobjektkategorie, Prozesse, Informationsarten oder – als dokumentierte Spezialisierung – ein konkretes Objekt beziehen. Je Szenario wird festgelegt, welche Schutzziele berührt sind und ab wann der Schaden „normal“ oder „hoch“ ist.				
SZENARIO	BEZUG	SCHUTZZIELE	NORMAL	HOCH
Abfluss von Verbrauchs- und Vertragsdaten Meldepflicht nach DSGVO, Vertrauensverlust, Bußgeld	Informationsart	C	Einzelne Datensätze, keine besonderen Kategorien	Daten vieler Kundinnen und Kunden oder Zahlungsdaten
Fehlende Nachweise für Aufsicht und Eichrecht Beanstandung durch Aufsicht, Haftung der Leitung	Institution	TRACE	Lücke einzelner Protokolle, rekonstruierbar	Nachweis nicht rekonstruierbar
Manipulierte Schalthandlung oder Messwerte Anlagenschaden, Fehlabrechnung, Versorgungsunterbrechung	Prozess	AUTH, I	Auswirkung auf einzelne Messstellen, rückholbar	Wirkung auf Netzbetrieb oder viele Abrechnungen, nicht rückholbar
Ausfall der Leitstelle oder der Messdatenverarbeitung Gefährdung der Versorgung, Verletzung von Meldefristen, Vertragsstrafen	Prozess	A	Ausfall bis zu einem Arbeitstag, Ersatzverfahren verfügbar	Ausfall über die zulässige Wiederanlaufzeit hinaus

ABLEITUNGSREGELN			
Strukturierte Regeln ergänzen die allgemeinen Eskalations-/Deeskalationskriterien, sie ersetzen sie nicht. Es handelt sich um eine Festlegung der Institution, nicht um einen Verfahrensschritt des BSI-Standards 300-1.			
REGEL	TYP	SCHUTZZIEL	PFLICHTEN
Manuelles Ersatzverfahren erprobt	Deeskalation	alle	Begründung, Genehmigung, Review
Daten öffentlich oder bereits veröffentlicht	Deeskalation	alle	Begründung, Genehmigung, Review
Kumulation: viele Betroffene gleichzeitig	Eskalation	alle	Begründung, Review
Gesetzliche Meldefrist oder Aufsichtspflicht	Eskalation	alle	Begründung, Review
Gefahr für Leib und Leben	Eskalation	alle	Begründung, Review

- ✓
- Eigene Schutzziele neben C, I und A: im Beispiel Authentizität (AUTH) und Nachvollziehbarkeit (TRACE)

Leitlinie und Dokumente.

Die Leitlinie mit Versionen, Freigabe durch die Leitung und Nachweis der Kommunikation. Alle ISMS-Dokumente mit Freigaben an einem Ort.

Leitlinie

Diese Gruppe enthält die Sicherheitsleitlinie und ihre Kommunikationsbestätigung.

Letzte Freigabe

Aktueller Entwurf

Schreibgeschützt — dies ist die freigegebene Version.

LEITLINIENGRUPPE FREIGEBEN

Freigegeben

Freigegeben am 28.10.2026, nächste Review fällig am 2027-10-28.

Kommunikationsstand der freigegebenen Leitlinie

Bestätigen Sie je freigegebener Fassung, an welchem Tag sie an alle Mitarbeitenden kommuniziert wurde.

Leitlinie v2 freigegeben 28.10.2026

Kommunikation am 28.10.2026 bestätigt durch Kim Nordstern.

Kommuniziert

Leitlinie v1 freigegeben 12.7.2026

Kommunikation am 1.8.2026 bestätigt durch Kim Nordstern.

Kommuniziert

Register

Titel	Art	Version	Status	Klassifikation	Nächstes Review	Aufbewahrung bis
Informationssicherheitsleitlinie der Nordstern Stadtwerke	Leitlinie und Richtlinie	v2	Veröffentlicht	Offen	28.10.2027	28.10.2036
Notfallhandbuch Netzleitstelle	Konzept	v2	Veröffentlicht	Vertraulich	28.10.2027	28.10.2036
Richtlinie Datensicherung und Wiederherstellung	Leitlinie und Richtlinie	v2	Freigegeben	Intern	28.10.2027	28.10.2036
Richtlinie Kryptografie und Schlüsselverwaltung	Leitlinie und Richtlinie	v2	Veröffentlicht	Intern	28.10.2027	28.10.2036
Richtlinie Lieferantenmanagement	Leitlinie und Richtlinie	v1	Entwurf	Intern	—	—
Richtlinie Zugriffssteuerung und Berechtigungen	Leitlinie und Richtlinie	v2	Veröffentlicht	Intern	28.10.2027	28.10.2036
Verfahren Sicherheitsvorfälle melden und bewältigen	Verfahrens- und Arbeitsanweisung	v2	Veröffentlicht	Intern	26.04.2027	28.10.2031
Verfahren Änderungsmanagement	Verfahrens- und Arbeitsanweisung	v1	In Prüfung	Intern	—	—

Die Leitung setzt die Regel.

Statt jedes Restrisiko einzeln zu entscheiden, legt sie für jede Zelle der Risikomatrix fest: automatisch akzeptieren, einzeln entscheiden oder ablehnen.

Wahrscheinlichkeit ↓ / Auswirkung →	Vernachlässigbar	Gering	Spürbar	Erheblich	Existenzbedrohend
Sehr häufig	5 · Mittel ⚙️ Manuell	10 · Hoch ⚙️ Manuell	15 · Hoch ⚙️ Manuell	20 · Kritisch 🚫 Ablehnen	25 · Kritisch 🚫 Ablehnen
Häufig	4 · Gering ✓ Automatisch	8 · Mittel ⚙️ Manuell	12 · Hoch ⚙️ Manuell	16 · Hoch ⚙️ Manuell	20 · Kritisch 🚫 Ablehnen
Gelegentlich	3 · Gering ✓ Automatisch	6 · Mittel ⚙️ Manuell	9 · Mittel ⚙️ Manuell	12 · Hoch ⚙️ Manuell	15 · Hoch ⚙️ Manuell
Selten	2 · Gering ✓ Automatisch	4 · Gering ✓ Automatisch	6 · Mittel ⚙️ Manuell	8 · Mittel ⚙️ Manuell	10 · Hoch ⚙️ Manuell
Sehr selten	1 · Gering ✓ Automatisch	2 · Gering ✓ Automatisch	3 · Gering ✓ Automatisch	4 · Gering ✓ Automatisch	5 · Mittel ⚙️ Manuell

- ✓ Grün, dicke Linie: vorab akzeptiert. Rot, gestrichelt: abgelehnt, dort braucht jedes Risiko Maßnahmen
- ✓ Die runde Zahl zeigt, wie viele Risiken nach Maßnahmen heute in der Zelle liegen
- ✓ Wer jedes Restrisiko einzeln freigeben will, stellt das mit einem Schalter ein

Ausnahmen bleiben möglich, aber befristet.

Liegt ein Risiko in einer gesperrten Zelle, beantragt der Risikoeigentümer eine Ausnahme mit Begründung und kompensierenden Maßnahmen. Die Leitung entscheidet, mit Frist und Auflagen.

▼ Zahlungsabwicklung ohne Ende-zu-Ende-Verschlüsselung

Zelle des Restrisikos

⊗ Ablehnen · Sehr häufig / Erheblich

Antragsteller

Risikoeigentümer

Beantragt am

28.10.2026

Befristung

bis 25.04.2027

⌚ Offen

.....

Entscheidende Rolle

Institutionsleitung / Geschäftsführung

Begründung der Entscheidung (Pflicht)

Genehmigt bis ⓘ

25.04.2027

📅

Genehmigt bis 25.04.2027

Beantragt war 25.04.2027; spätestens 28.10.2027 (Mindestkriterium 28).

↔ Institutionelle F

Genehmigt bis ⓘ

25.04.2027

📅

Genehmigt bis 25.04.2027

Beantragt war 25.04.2027; spätestens 28.10.2027 (Mindestkriterium 28).

Auflagen (optional) ⓘ

auswählen ▼

Genehmigen

Ausschnitt vergrößert

Auflagen

1. Migration bis zum Ende der Befristung abschließen; Terminplan der Institutionsleitung monatlich berichten.

2. Kompensierende Maßnahmen (Segmentierung, Jump-Host, Protokollauswertung) bis dahin lückenlos betreiben und nachweisen.

3. Bei einem Sicherheitsvorfall am Leitrechner oder bei neu bekannt gewordenen Schwachstellen ist die Genehmigung unverzüglich zu überprüfen.

Befristung nach Anhang 3, Kriterium 28. In der App höchstens ein Jahr.

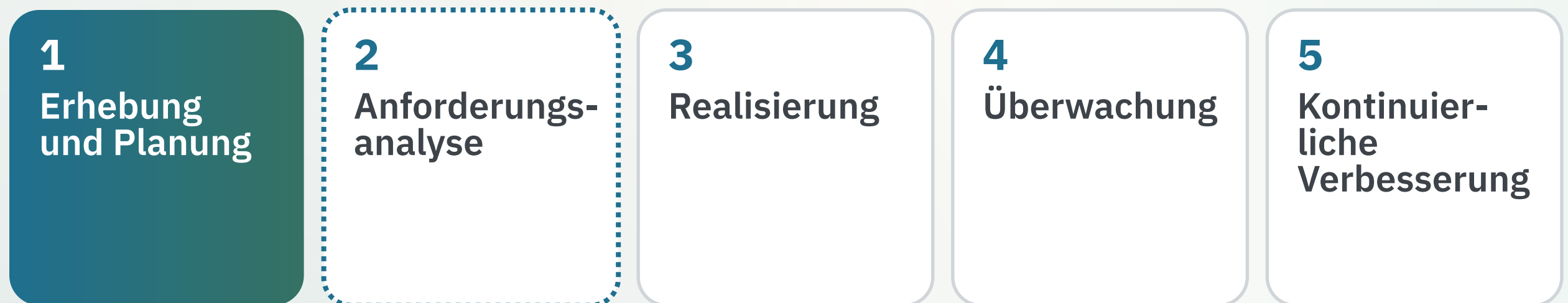
 BlueProceedings ISMS für Grundschutz++ · Pre-Alpha, Demodaten

13 / 15

Verteilt erfassen. Zentral steuern. Einmal freigeben.

Fachbereiche liefern, der ISB steuert, die Leitung entscheidet über Regeln statt über jeden Einzelfall. Die Verantwortung bleibt, wo der Standard sie verlangt.

NÄCHSTER BEITRAG: SCHRITT 2



Testphase ab 11.11.2026

Bis zu elf Personen aus der ISMS-Praxis. Alle Funktionen und die Bewerbung auf **blueproceedings.de**.

Danke fürs Lesen!

BlueProceedings ISMS entsteht in meiner Freizeit, made in Germany, aus der ISMS-Praxis für die ISMS-Praxis. Hinter dem Projekt steht kein Werbebudget. Deshalb bitte ich euch um Unterstützung:

1

Teilen

den Beitrag mit allen, die gerade an Grundschutz++ arbeiten.

2

Folgen

der Seite von BlueProceedings. Dort geht es mit Schritt 2 weiter.

Mich interessiert:

Wie löst ihr die Teilschritte von Schritt 1 momentan? Und vor allem: Gibt eure Leitung jedes Risiko frei, unabhängig von seiner Bewertung? Ich freue mich über Erfahrungen und Widerspruch.

Mehr dazu

Methodik in fünf Schritten
Projekt ansehen
Testphase ab 11.11.

Neuigkeiten

blueproceedings.de/bsi-standard-300-1
blueproceedings.de
blueproceedings.de/#download
bis zu elf Personen, Bewerbung per E-Mail
linkedin.com/company/blueproceedings

