

eco e.V. – Verband der Internetwirtschaft 17.10.2024

Leitungsgorgane unter NIS2-Bedingungen

.....

ULRICH PLATE

nGENn

TAILORED CONCEPTS



Leitungsgorgane unter NIS2



Letztverantwortung und persönliche Haftung



Keine Delegation von Pflichten

Beauftragung eines Dritten zur Umsetzung und Überwachung ist nicht zulässig – auch nicht horizontal an einen Cybersicherheitsvorstand o.ä.



Compliance-Verantwortung

Verteilung von Aufgaben der IT-Sicherheit kein Problem, aber Letztverantwortung verbleibt immer in der Geschäftsleitung



Persönliche Haftungsrisiken

- Kosten des Ausfalls
- Bußgelder
- Lösegeldzahlungen
- Vertragsstrafen, Schadenersatz
- Zusatzkosten für externe Dienstleister (Rechtsberatung, Forensik)



Anspruchsverzicht unwirksam

Aktueller Gesetzentwurf etwas entschärft, aber Ersatzansprüche gegen die Geschäftsleitung gesellschaftsrechtlich nicht verzichtbar. D&O-Versicherungen aber vermutlich weiter zulässig.



Cybersicherheit ist Chefsache



Unmittelbar resultierende Verpflichtungen



Meldeverfahren für „erhebliche Sicherheitsvorfälle“



„Frühwarnung“

wenn möglich mit Hinweis auf etwaige kriminelle Ursachen und/oder grenzüberschreitende Auswirkungen

Meldung

mit Bewertung von Schweregrad und Auswirkung

Bericht

mit Informationen über ergriffene Abwehrmaßnahmen (abgeschlossen oder andauernd)



Explizite Anforderungen an die Leitungsgorgane



Pflicht der Geschäftsleitung zur regelmäßigen Schulung



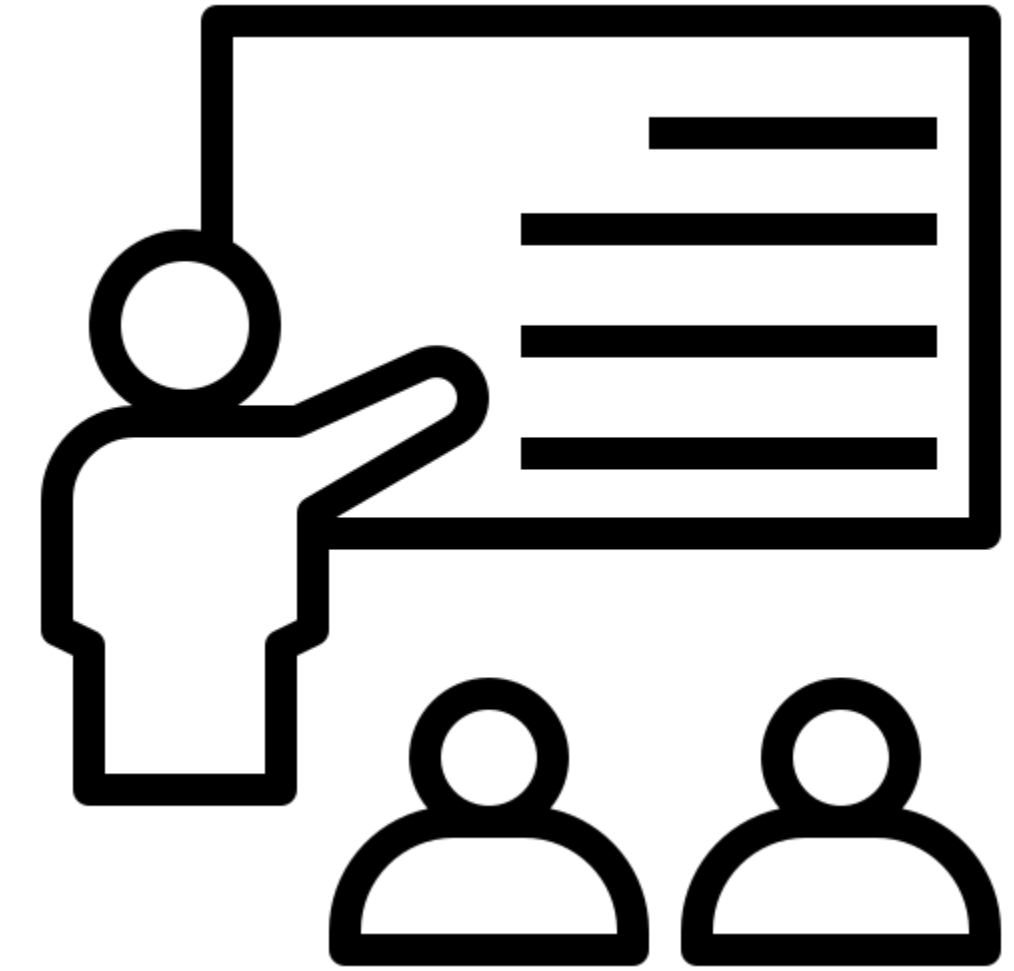
Umsetzung

Geschäftsleitungen müssen die zu ergreifenden Risikomanagementmaßnahmen umsetzen...



Überwachung

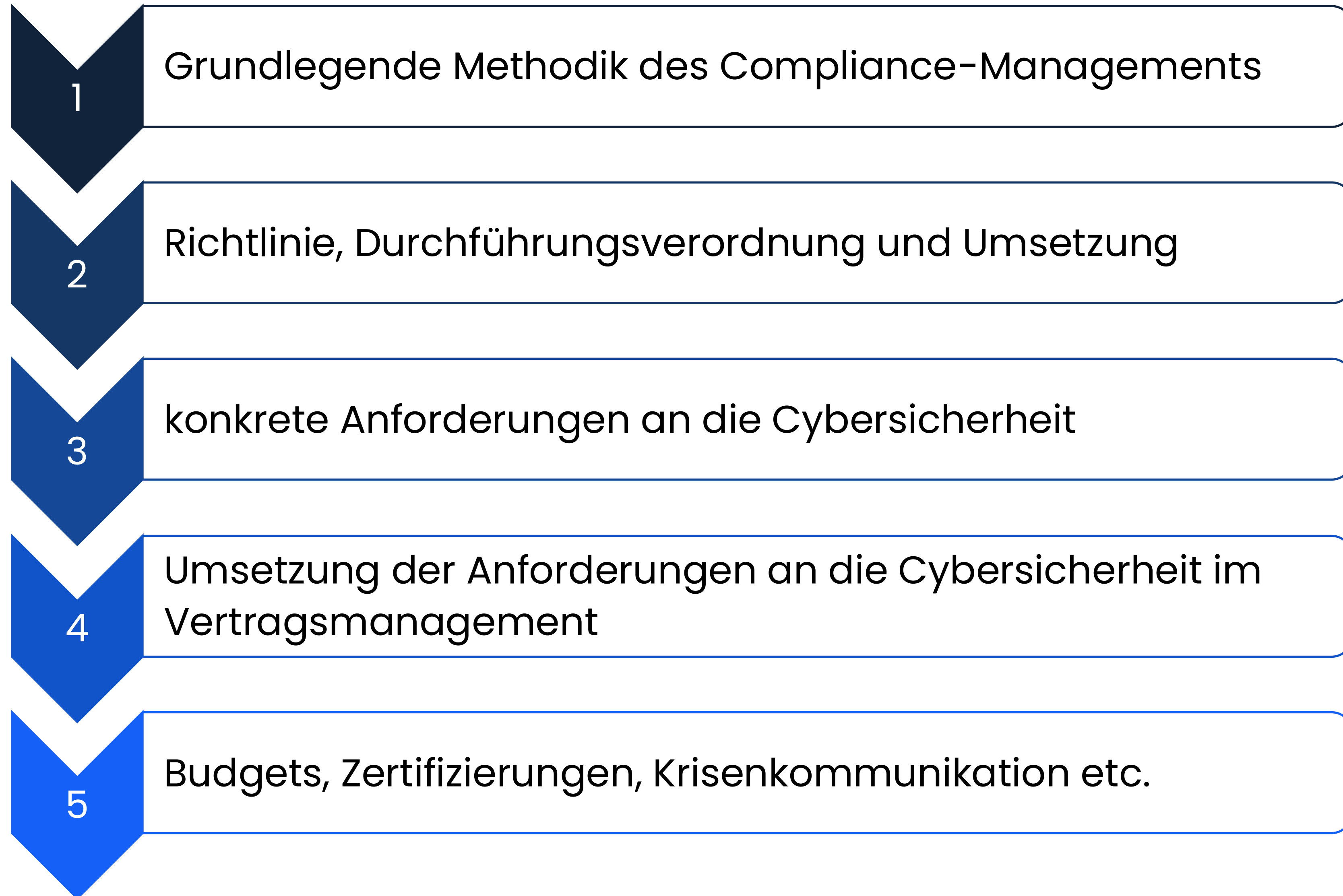
...und ihre Umsetzung überwachen



Schulung

Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken erwerben

Geschäftsleitungsschulungen nach § 38 (3)



Art. 20 NIS2 Billigung ↔ Umsetzung § 38 BSI-G neu

Risikomanagementmaßnahmen

Richtlinie fordert die Billigung der zur Einhaltung von Art. 21 erforderlichen Mindessicherheitsanforderungen

NIS2UmsuCG geht über „billigen“ hinaus und fordert „umsetzen“

Beide verlangen die Überwachung der Umsetzung durch die Leitungsgorgane



Compliance-Methodik



Compliance-Management



Compliance in alle Richtungen

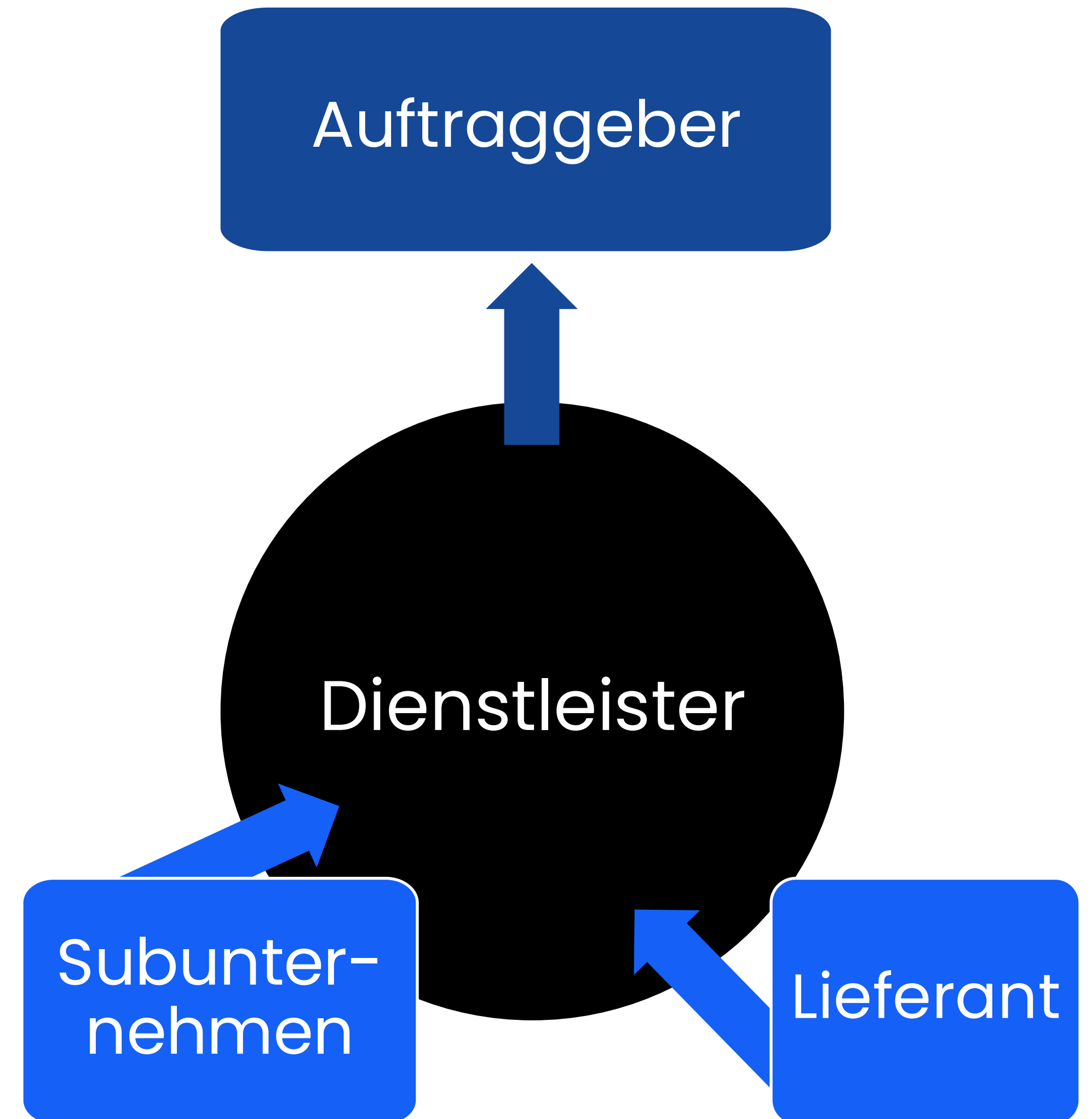
Kunden / Auftraggeber sind nach NIS2 und / oder KRITIS-DachG verpflichtet



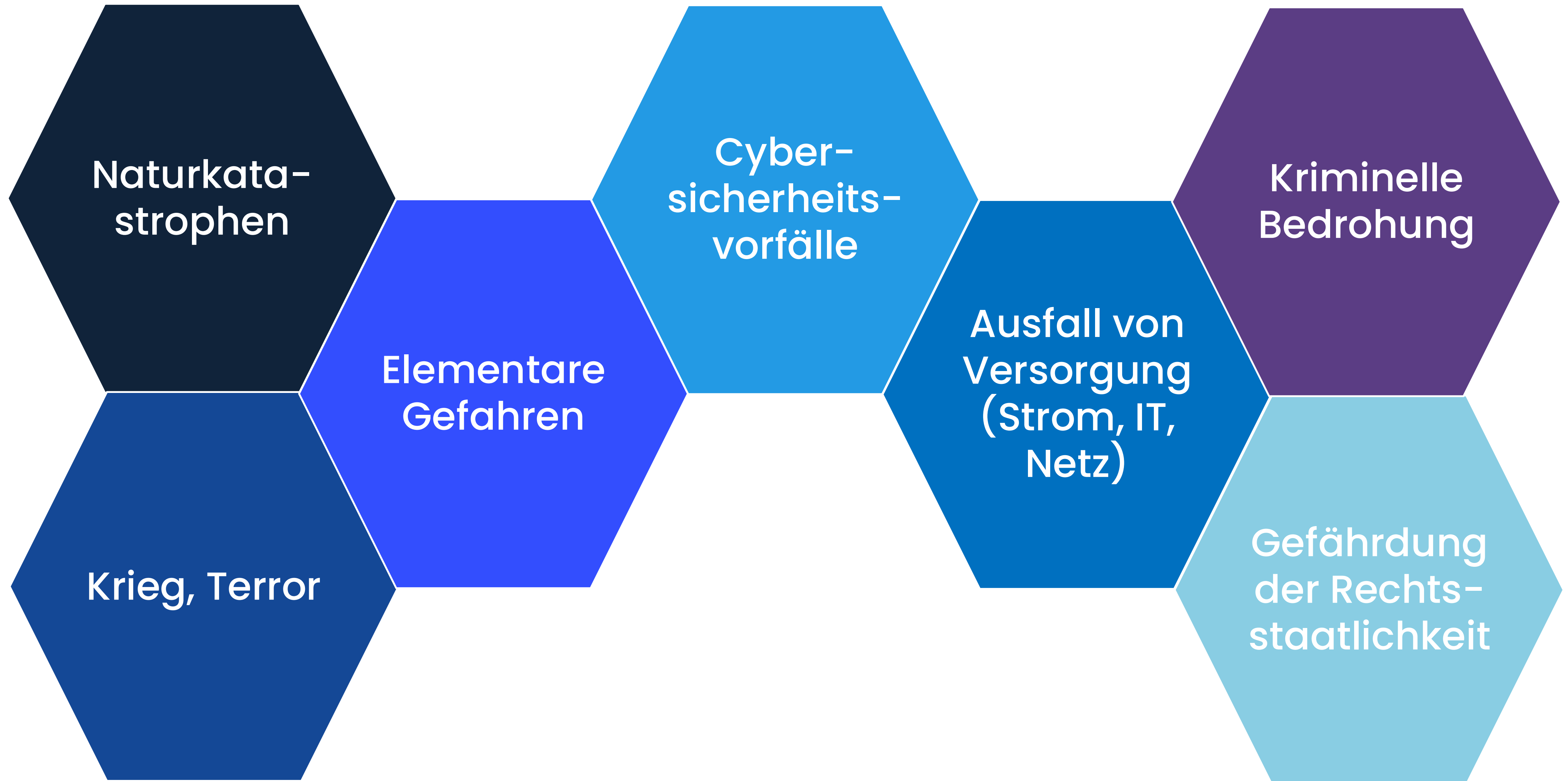
Kunde verlangt vom Dienstleister vertragliche Zusagen der Vorgaben



Dienstleister ist selbst der Regulierung durch NIS2 / KRITIS-DachG unterworfen



All hazards approach



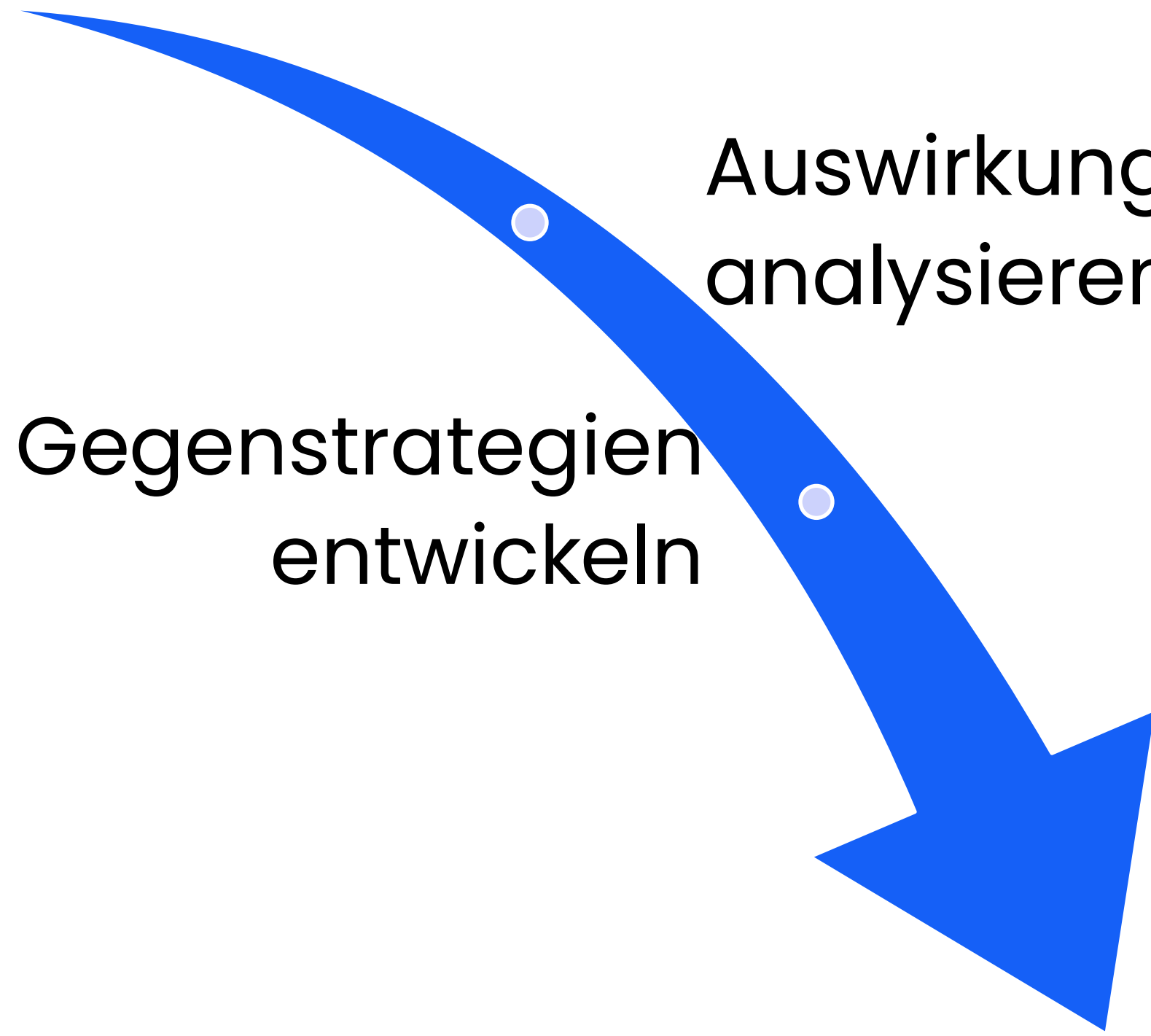
Cyber Risiken identifizieren und behandeln

Erkannte
Bedrohungen

Auswirkungen
analysieren

Gegenstrategien
entwickeln

Systemische
Resilienz



Risikomanagementsystem

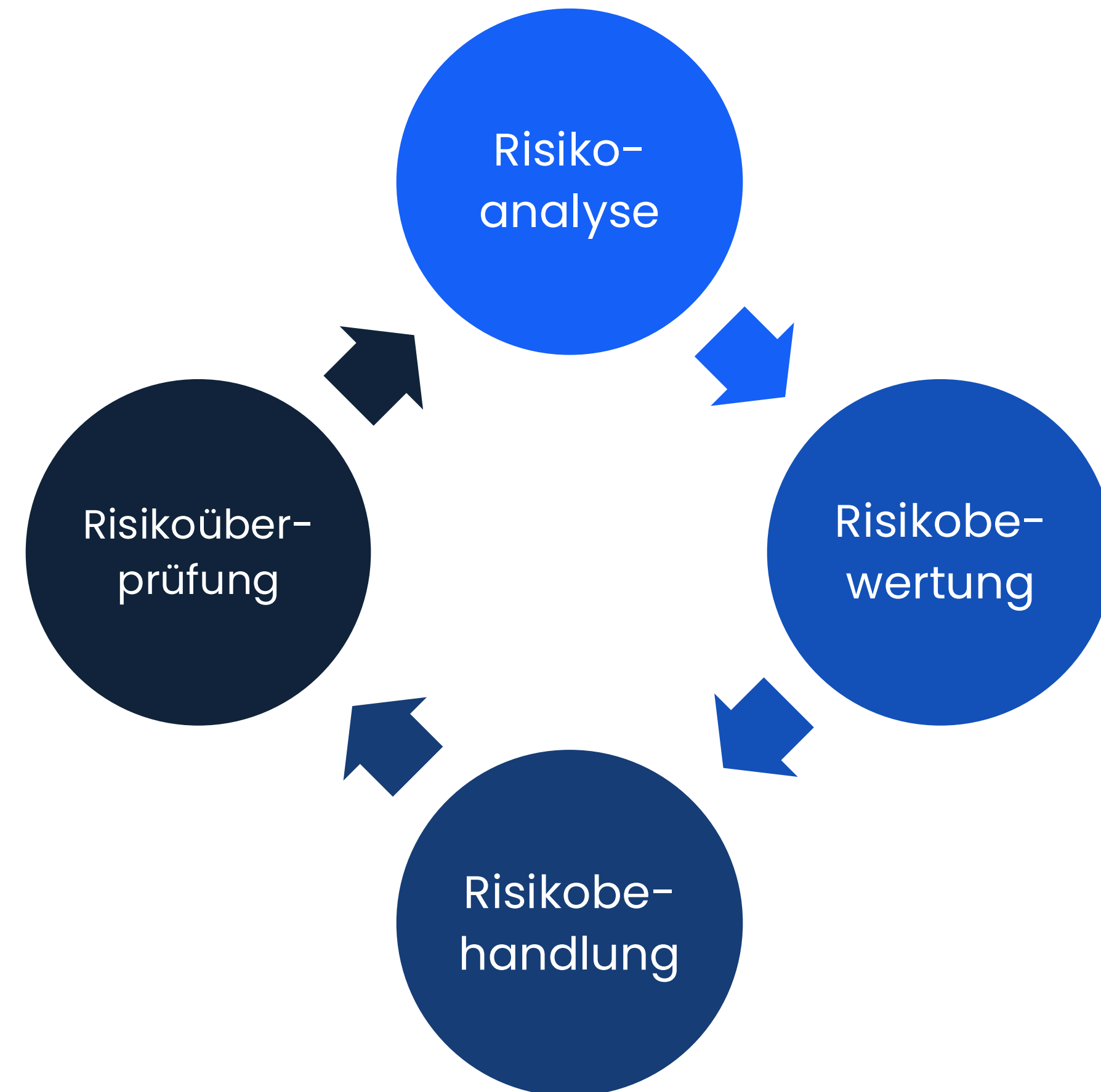
KonTraG

StaRUG

CSRD

...

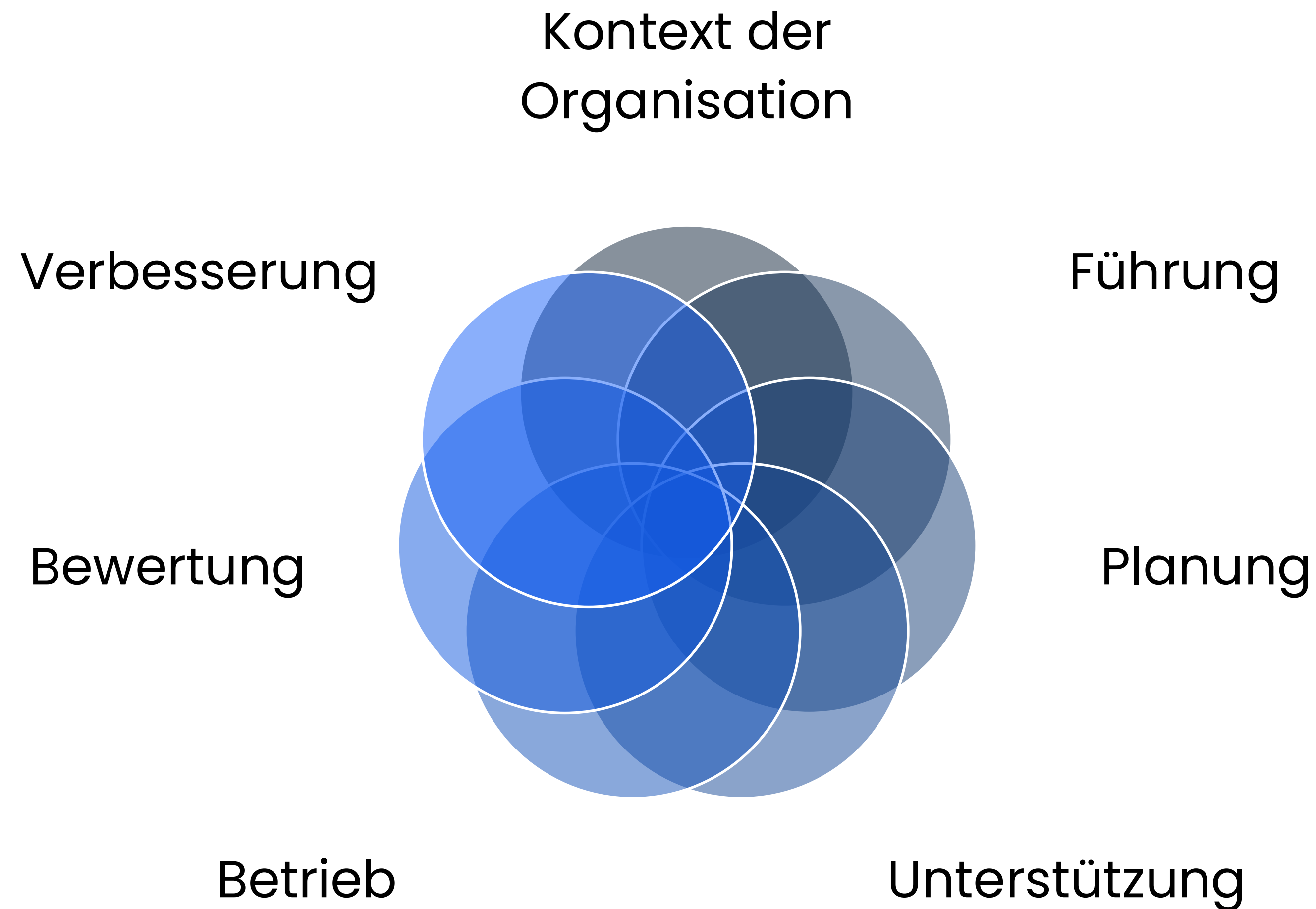
Gesetzliche
Verpflichtungen zu
Risikomanagement



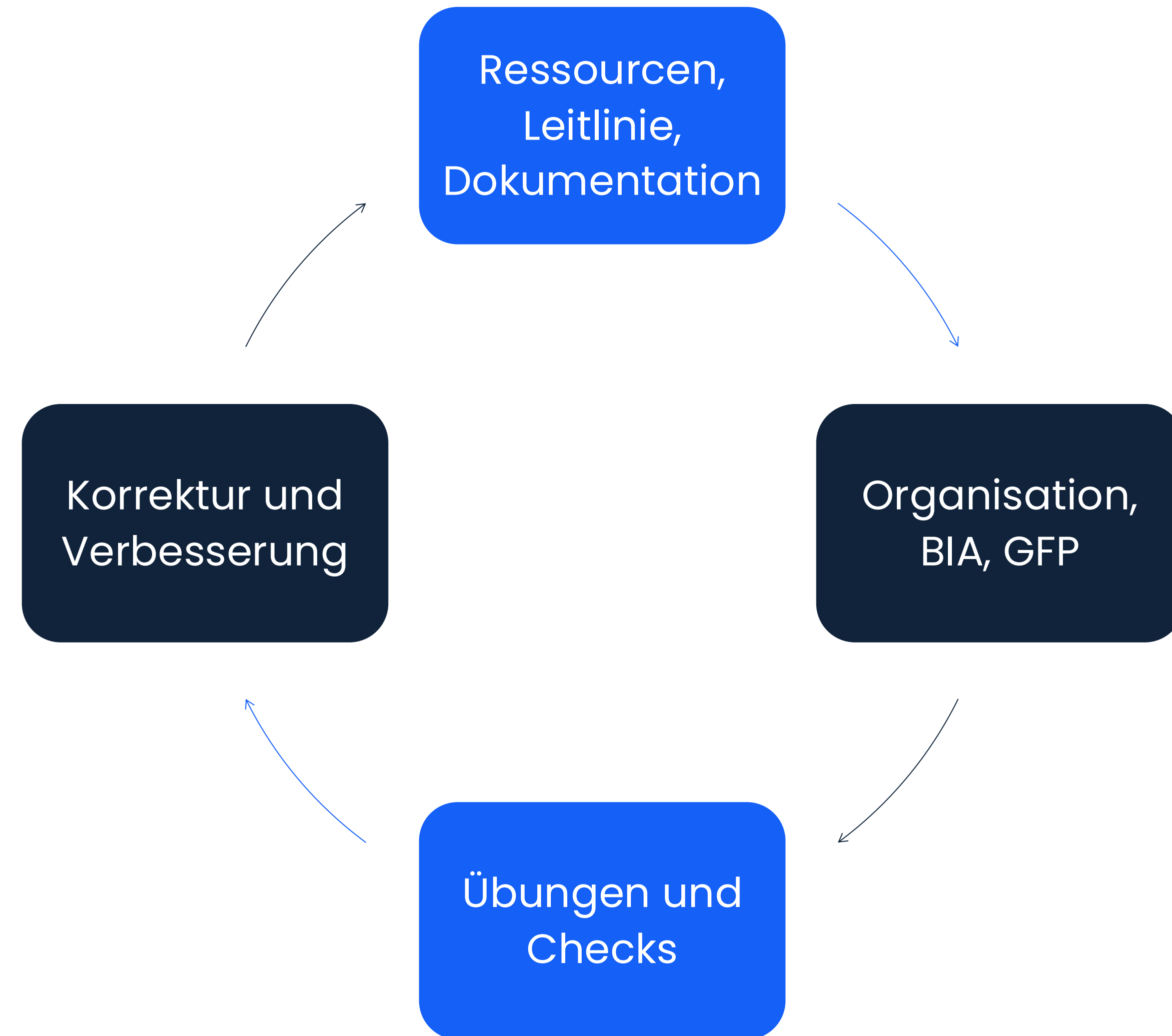
Risikomanagement für Betreiber kritischer Anlagen



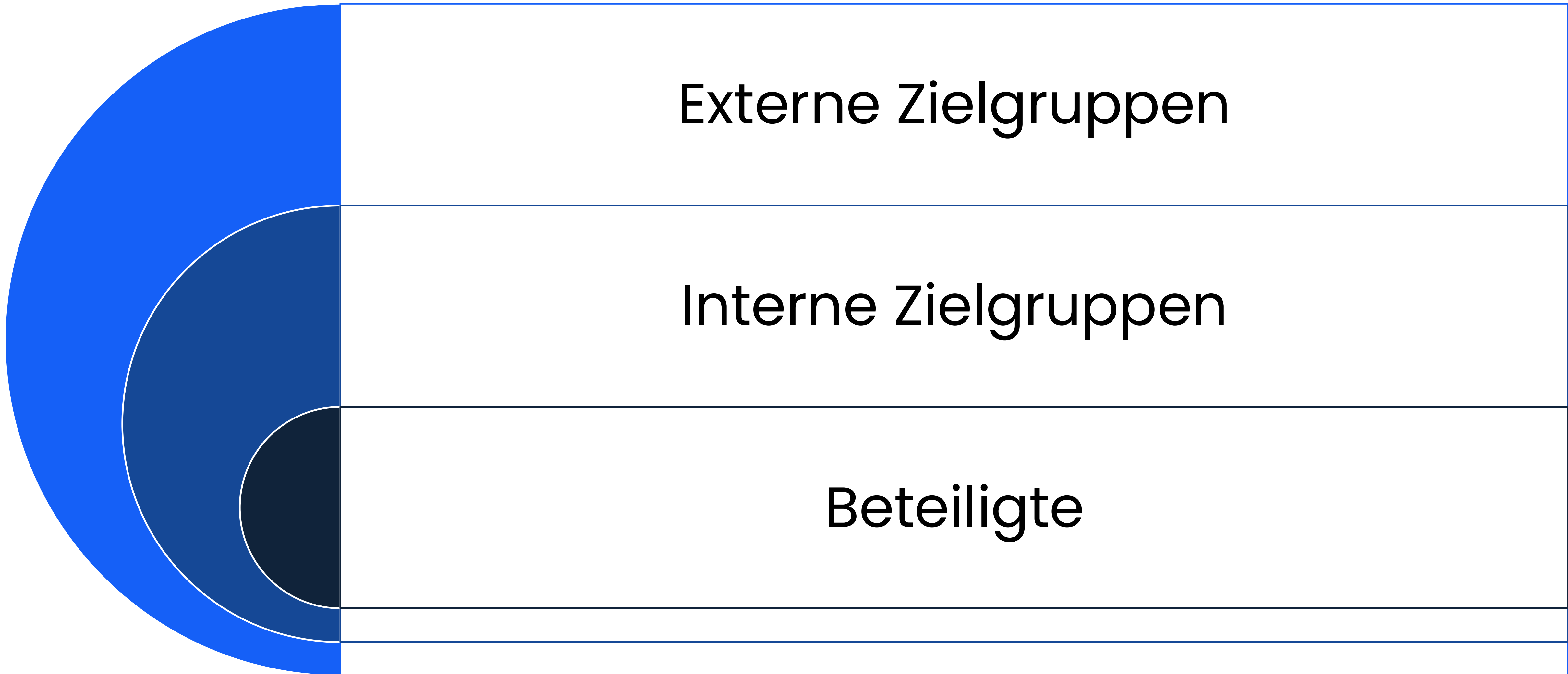
Informationssicherheitsmanagement



Business Continuity Management



Krisenkommunikation und -management





Richtlinie, Verordnung, Gesetz



NIS2, Durchführungsverordnung und Umsetzungsgesetz



Überblick, Inhalte, Einordnung

Risikomanagementmaßnahmen nach Katalog der Mindestsicherheitsanforderungen, Melde- und Registrierungspflicht



Anwendungsbereich, Kategorien

Mehr Sektoren, size-cap-rule, wichtige und besonders wichtige Einrichtungen, Betreiber kritischer Anlagen



Direkte und indirekte Betroffenheit

Direkte Verpflichtung als reguliertes Unternehmen, aber Durchgriff auf Lieferantenverhältnisse



Stand und Besonderheiten in DE

Rolle des BSI als Zentralstelle; Kritis-VO unverändert, aber unter neuem Gesetz



Abgrenzung zu DORA, CER, CRA...

Besondere Regeln für Finanzmarktinstitutionen, physische Sicherheit kritischer Anlagen, Komponenten



Regulierungsgefüge verstehen

Welche Regeln für welche Unternehmen in welchen Branchen und für welche Anwendungen?



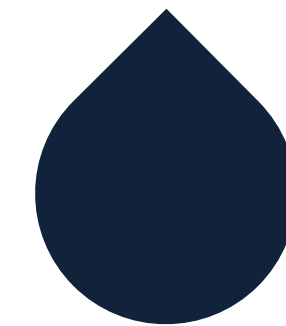
Konkrete Sicherheitsanforderungen



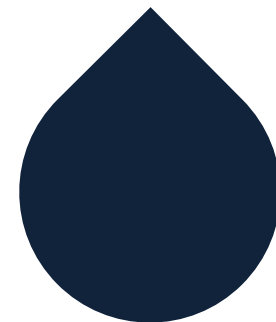
Katalog der Mindestanforderungen (§ 30 (2) 1–10)



Risikoanalyse und Informationssicherheit



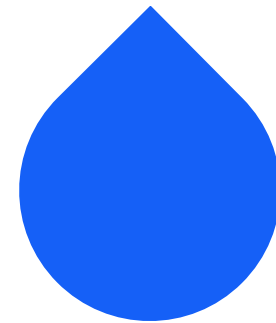
Bewertung von Risikomanagement



Bewältigung von Sicherheitsvorfällen



„Cyberhygiene“ und Schulungen



Business Continuity Management



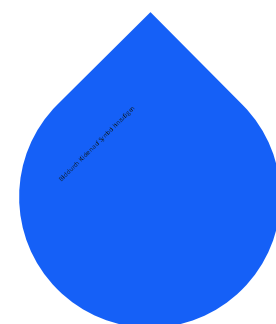
Kryptografische Verfahren



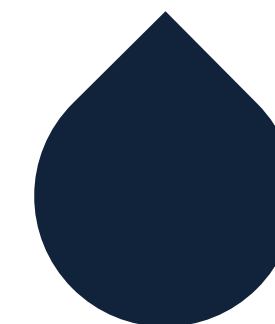
Lieferkettensicherheit



Personal, Zugriffskontrolle, Assets



Beschaffungs- und Entwicklungssicherheit



MFA und gesicherte Kommunikation



Anwendungsbereich und Kategorien



„Size cap rule“ in NIS 2



Große Unternehmen
> 250 MA, > 50 Mio. Umsatz

Mittlere Unternehmen
> 50 MA, > 10 Mio. Umsatz

Kleine und
Kleinstunternehmen

Besonders
wichtige
Einrichtungen




- Große Unternehmen aus den Sektoren in Annex I
- Mittlere TK-Anbieter/ISPs
- diverse Sonderfälle

Wichtige
Einrichtungen

- Mittlere Unternehmen aus den Sektoren in Annex I
- Große und mittlere Unternehmen aus Annex II

Abweichende Kategorien für digitale Dienste

Digitale Dienste	> 250 MA und 50 Mio. € Umsatz	> 50 MA und 10 Mio. € Umsatz	Kleinst- und Kleinunternehmen
DNS			
TLD-Register			
Qualifizierte Vertrauensdienste			
Öffentliche Kommunikationsnetze-/-dienste			
IXP			
Cloud-Computing-Dienste			
Rechenzentren			
Inhaltszustellnetze (CDN)			
Nichtqualifizierte Vertrauensdienste			

-  Besonders wichtige Einrichtungen
-  Wichtige Einrichtungen
-  Nicht im Anwendungsbereich

Von „kritischer Infrastruktur“ zu „kritischen Anlagen“

BSI-KritisV

„KRITIS“ nach
Sektoren, Anlagen-
kategorien und
Schwellenwerten

NIS2

„Betreiber kritischer
Anlagen“ als Unter-
kategorie „beson-
ders wichtiger Ein-
richtungen“, bei
noch unveränderter
Systematik



Sicherheit in der Lieferkette



Rechtliche Prüfung und Anpassung der Verträge





Chefsachen



Leitungsaufgaben

Budgetallokation
(„Cyberquote“)

Zertifizierungen

Nicht ausreichend
beherrschte
Risiken gezielt

Cyberversiche-
rungen nicht für
kritische Dienste

Krisenkommuni-
kation gegen
Reputations-
schäden

Übereinstimmung NIS2 und ISO 27001

Nur NIS2: 18 Prozent

Nur ISO: 10 Prozent

Kongruent: 72 Prozent





Fragen

nGENn GmbH
Erdfunkstelle 1, 61250 Usingen
www.ngenn.net

nGENn



nGENn GmbH
Erdfunkstelle 1, 61250 Usingen
www.ngenn.net