

Konzern, KRITIS, KMU

Die Einstufung nach NIS-2 im öffentlichen Beteiligungsverbund

Kristian Borkert & Gianna Nobile

JURIBO Legal & Consulting



Herbstakademie 2026

Montag, 9:04 Uhr: ein Anruf aus Cloudingen

Der Kämmerer hat das Registrierungsportal des BSI offen – und keine Antwort



„Wir haben sieben Gesellschaften. Muss sich jede einzeln registrieren – oder reicht die Holding? Und was ist mit unserer IT-Tochter?“

Kämmerer der Stadt Cloudingen, 9:04 Uhr



Sind wir überhaupt betroffen?



Wer zählt bei der Größe alles mit?



Was ist mit unserer IT-Tochter?



Wer haftet am Ende persönlich dafür?

Und genau da beginnt das Problem: Keine dieser vier Fragen beantwortet das BSIG auf den ersten Blick.

Warum das kein Einzelfall ist

Fünf Monate nach Fristablauf fehlen noch rund 40 % der pflichtigen Unternehmen



17.945 von geschätzt 29.850
Stand 30.6.2026 · Frist war der 6.3.2026

20.658

öffentliche Unternehmen

1.248 Mrd. €

Umsatz, ~50 % Energie

Vom Sonderfall zum Massenphänomen

KRITIS-Betreiber bisher



1.173

NIS-2-pflichtig künftig



29.850

registriert am 2.4.2026



15.691

registriert am 30.6.2026



17.945

+ 2.254 Registrierungen in drei Monaten – die Lücke schließt sich, aber langsam.

Unsere These: Die Lücke ist kein Compliance-Problem, sondern ein Einstufungsproblem – und im Beteiligungsverband ist sie am größten.

Die vier Fragen – und wo wir sie beantworten

Aufbau des Vortrags entlang des Falls Cloudingen



01 Ausgangslage

„Sind wir überhaupt betroffen?“ – Verbundstrukturen und der Leitfall



02 Anwendungsbereich & Zurechnung

„Wer zählt bei der Größe mit?“ – KMU-Empfehlung und Ausnahme



03 IT-Organisation & Governance

„Was ist mit unserer IT-Tochter?“ – MSP, § 38 BSIG, Verträge



04 Prüfschema & Fazit

„Wie gehen wir konkret vor?“ – vier Schritte und zwei Weichen

01

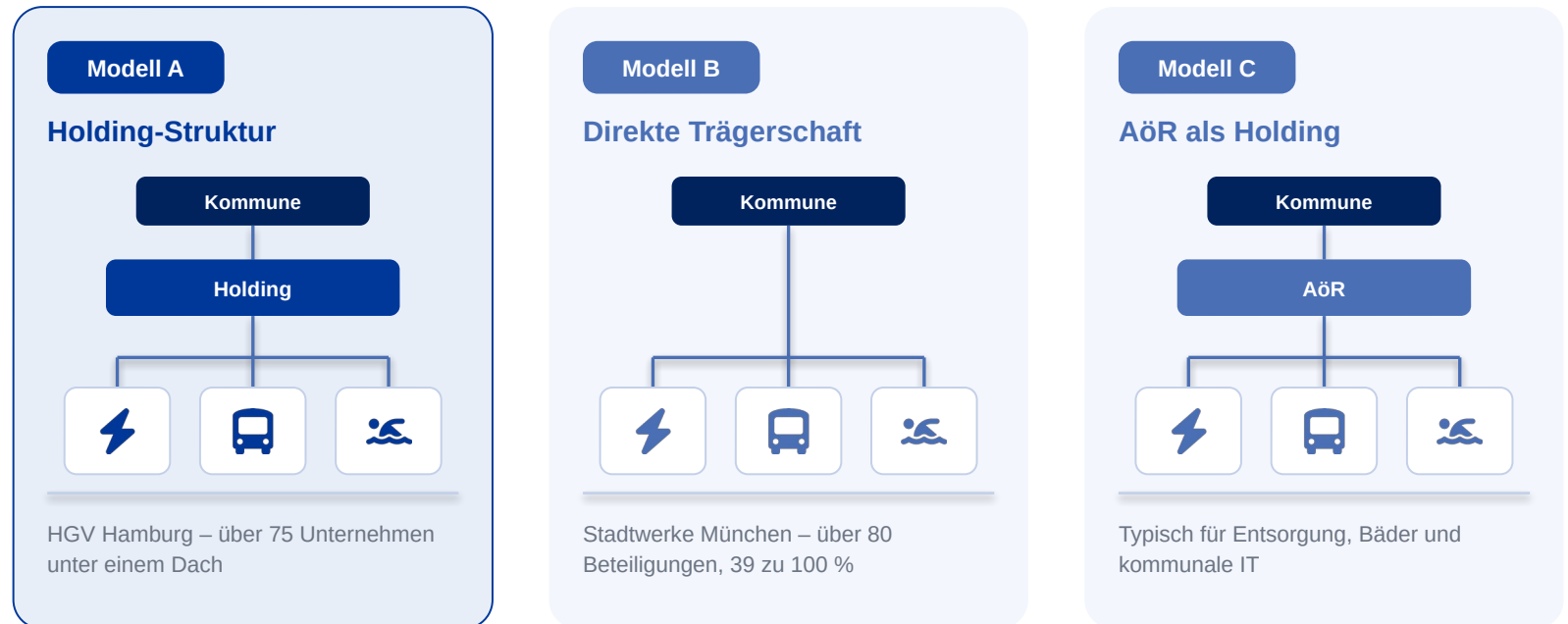
Ausgangslage

„Sind wir überhaupt betroffen?“



Wie die öffentliche Hand Daseinsvorsorge organisiert

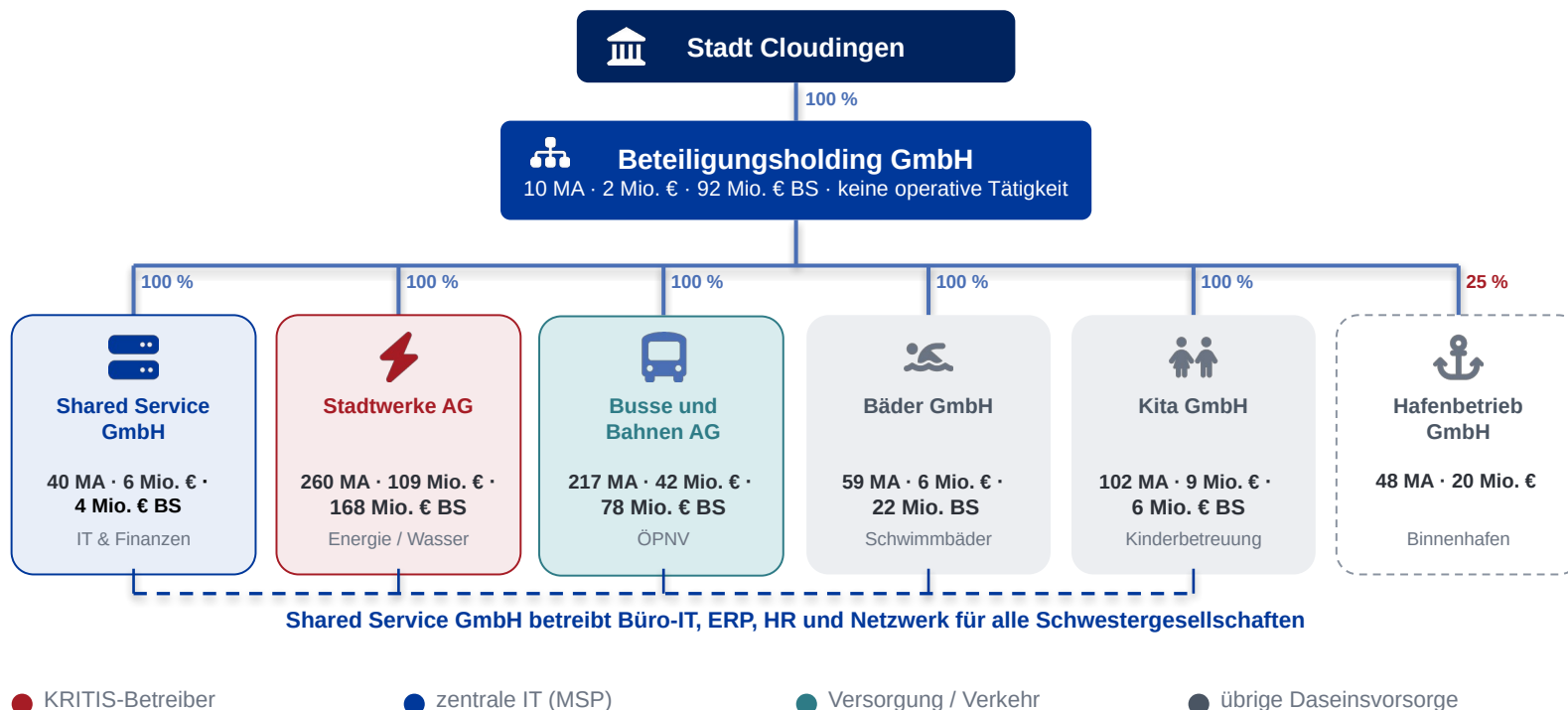
Art. 20 Abs. 1, Art. 28 Abs. 2 GG – drei Grundmodelle in der Praxis



Für heute: Wir arbeiten mit Modell A – Holding plus zentralem Shared Service. Der häufigste und regulatorisch heikelste Fall.

Der Fall: Modellkommune „Stadt Cloudingen“

Beteiligungsholding mit zentralem IT- und Finanz-Shared-Service

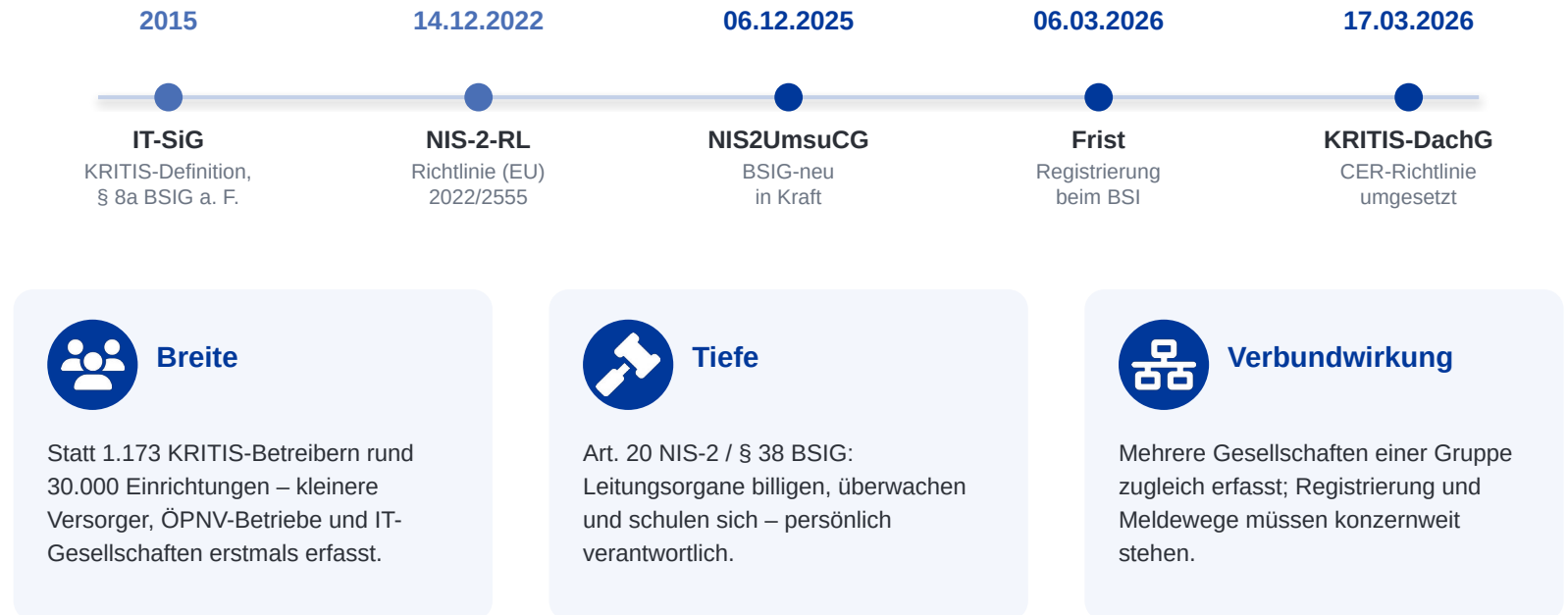


Die Architektur: Büro-IT und ERP zentral bei der Shared Service GmbH – die OT-Leittechnik der Stadtwerke bleibt strikt getrennt.

* MA = Mitarbeitende · OT = Operational Technology (Prozessleittechnik) · ERP = Enterprise Resource Planning · MSP = Managed Service Provider · gestrichelt = Minderheitsbeteiligung

Der Wendepunkt: von KRITIS zu NIS-2

Breite und Tiefe der Regulierung ändern sich gleichzeitig



Daneben, seit 17.3.2026: Das KRITIS-Dachgesetz setzt die CER-Richtlinie um und ergänzt die IT-Sicherheit um den physischen und organisatorischen Schutz. § 2 Nr. 22 und 24 BSIG verweisen für die kritische Anlage darauf.

Merksatz: NIS-2 ist kein größeres KRITIS. Es ist ein anderer Anknüpfungspunkt: die Einrichtung statt der Anlage.

* IT-SiG = IT-Sicherheitsgesetz · NIS2UmsuCG = NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz · KRITIS-DachG = KRITIS-Dachgesetz · CER = Critical Entities Resilience

02

Anwendungsbereich & Zurechnung

„Wer zählt bei der Größe eigentlich alles mit?“



Drei Gruppen – und zwei Schwellenwerte

§ 28 BSIG: KRITIS wird zur Zusatzqualifikation, nicht zum eigenen Regime



Schwellenwerte, § 28 Abs. 4 BSIG



Kein Konzernprivileg: Weder die Richtlinie noch das BSIG kennen eine Gesamtbetrachtung. Jede juristische Person wird einzeln geprüft.

* bwE = besonders wichtige Einrichtung · KRITIS = kritische Infrastrukturen

Zurechnung nach der KMU-Empfehlung 2003/361/EG

§ 28 Abs. 4 S. 1 BSIG – der Verbund rechnet sich in beide Richtungen zu



Lesart der Pfeile: Geprüft wird immer eine einzelne Gesellschaft. Hinzugerechnet werden nicht nur die Werte der Mutter, sondern deren konsolidierte Verbundwerte (Art. 6 Abs. 3 der Empfehlung der Kommission (2003/361/EG)).

Gesellschaft	Beteiligung	MA	Umsatz	Bilanzsumme	Größe direkt	nach Zurechnung
Beteiligungsholding GmbH	—	10	2 Mio. €	92 Mio. €	klein	Kein KMU
Shared Service GmbH	100 %	40	6 Mio. €	4 Mio. €	klein	Kein KMU
Stadtwerke AG	100 %	260	109 Mio. €	168 Mio. €	Kein KMU	Kein KMU
Busse und Bahnen AG	100 %	217	42 Mio. €	78 Mio. €	mittel	Kein KMU
Bäder GmbH	100 %	59	6 Mio. €	22 Mio. €	mittel	Kein KMU
Kita GmbH	100 %	102	9 Mio. €	6 Mio. €	mittel	Kein KMU
Verbundene Unternehmen gesamt		688	174 Mio. €	370 Mio. €	—	Schwellen überschritten
Hafenbetrieb GmbH (Partner)	25 %	48	20 Mio. €	n. b.	mittel	220 MA / 63,5 Mio. €

Zwischenergebnis: Ohne Ausnahme wäre jede Gesellschaft Großunternehmen – auch die Kita mit 102 Beschäftigten. Beim Hafen wirken 25 % in beide Richtungen.

* MA = Mitarbeitende · KMU = kleine und mittlere Unternehmen · n. b. = im Leitfall nicht bestimmt

Die IT-Unabhängigkeitsausnahme, § 28 Abs. 4 S. 2 BSIG

Deutscher Sonderweg mit Rückhalt in ErwG 16 NIS-2-RL



Entscheidet die Einrichtung eigenverantwortlich über Beschaffung, Betrieb und Konfiguration ihrer IT-Systeme?

Maßstab: Nicht wer die IT betreibt, sondern wer über sie bestimmt. (Konkret: „über die rechtlichen, wirtschaftlichen & tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse“)



JA Unabhängig

Die IT wird an einen Dienstleister ausgelagert – der bestimmende Einfluss bleibt über den Outsourcing-Vertrag erhalten.

Im Leitfall: ausgelagert, aber über den Vertrag gesteuert

Nur die Eigenwerte zählen



NEIN Nicht unabhängig

Sämtliche IT-Systeme werden zentral von der Konzernmutter betrieben; die Einrichtung kann faktisch keinen Einfluss nehmen.

Variante: Holding beherrscht die Töchter – kein Vertrag wirkt

Verbundwerte werden voll zugerechnet

Nur in klaren Fällen: Die Ausnahme trägt, wo die IT-Autonomie vertraglich belegt ist. Bleibt ein Zweifel, ist voll zuzurechnen – Rechtsprechung fehlt, das BSI dürfte eng auslegen.

* ErwG = Erwägungsgrund · BSI = Bundesamt für Sicherheit in der Informationstechnik

Die Auflösung: Einstufung im Verbund Cloudingen

Dasselbe Bild wie am Anfang – jetzt mit der Antwort für den Kämmerer



Bäder GmbH und Kita GmbH

Beide erscheinen weder in Anlage 1 noch in Anlage 2 BSIG. Die Prüfung endet schon bei Schritt 1 – auf die umstrittene Ausnahme des § 28 Abs. 3 BSIG kommt es nicht an.

Hafenbetrieb GmbH

Erfasst nur als Leitungsorgan eines Hafens i. S. d. RL 2005/65/EG. Eigene 20 Mio. € reichen für „wichtig“; für bwE fehlt es an 250 MA. Dann entscheidet § 28 Abs. 1 Nr. 4 BSIG – und damit die Bilanzsumme, die der Leitfall offenlässt.

Die Antwort: Zwei Gesellschaften sind sicher reguliert, eine ist es nur unter Vorbehalt – nicht der ganze Verbund. Die Zurechnung entscheidet, nicht die Konzernzugehörigkeit.

* bwE = besonders wichtige Einrichtung · MSP = Managed Service Provider (Anlage 1 Nr. 6.1.10 BSIG) · MSSP = Managed Security Service Provider (Nr. 6.1.11)

Vier offene Flanken der deutschen Umsetzung

Wo die Beratung heute das Risiko sensibel steuern muss



Vernachlässigbare Geschäftstätigkeiten

§ 28 Abs. 3 BSIG

Ohne Entsprechung in der NIS-2-RL. Verengt den persönlichen Anwendungsbereich und dürfte unionsrechtswidrig sein. Im Leitfall kommt es darauf nicht an.

Folge: Wer sich darauf stützt, riskiert die spätere Einstufung.



MSP und MSSP

Anlage 1 BSIG

Der deutsche Katalog nennt unter 6.1.10 / 6.1.11 Begriffe, die Annex I nicht kennt. Zu lösen über effet utile und richtlinienkonforme Auslegung.

Folge: Jede konzerninterne IT-Gesellschaft prüfen.



Unabhängigkeitskriterien

§ 28 Abs. 4 S. 2 BSIG

Keine Rechtsprechung, keine belastbare Verwaltungspraxis des BSI. Bis dahin ist die vorsichtige Auslegung geboten.

Folge: Einstufung revisionsfest dokumentieren.



Kommunale Eigenbetriebe

§ 28 Abs. 4 S. 1 BSIG

Rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft sind ausdrücklich ausgenommen. Offen bleibt, welche Werte stattdessen zählen.

Folge: Bis zu einer BSI-Leitlinie nur Eigenwerte ansetzen und begründen.

Beratungsfolge: Wer heute einstuft, dokumentiert die Begründung – jede der vier Flanken kann die Einstufung nachträglich kippen.

* MSP = Managed Service Provider · MSSP = Managed Security Service Provider · KMU = kleine und mittlere Unternehmen

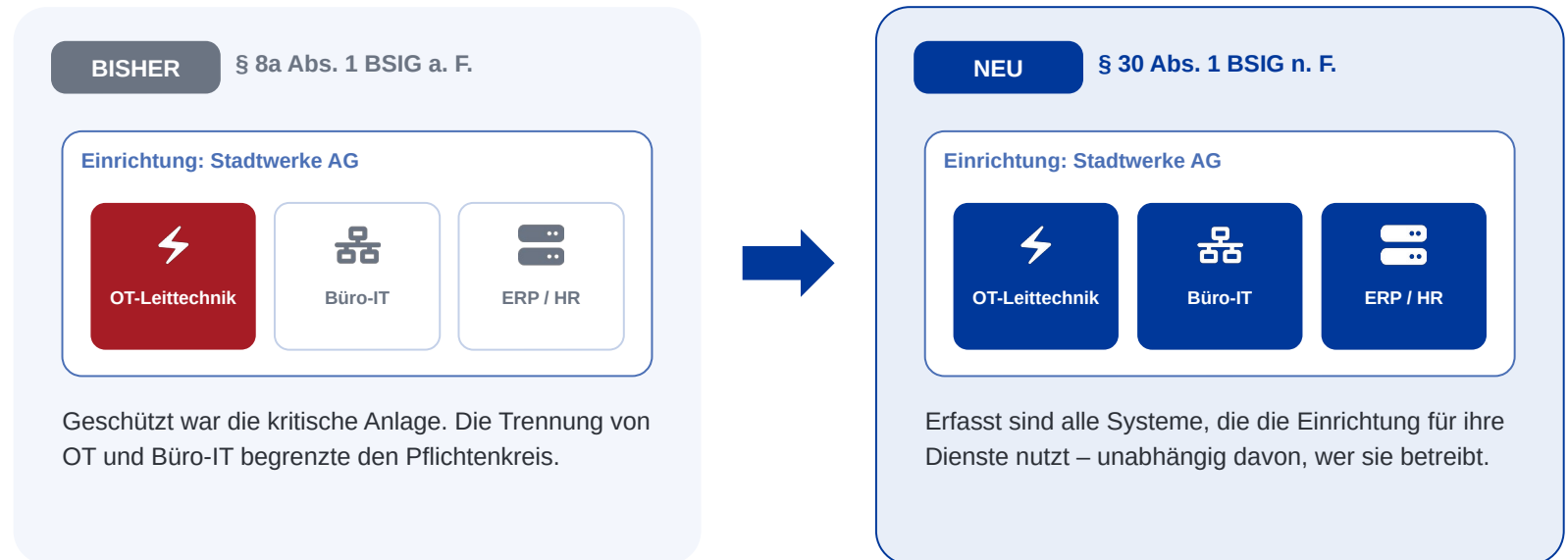
03

IT-Organisation & Governance

„Was ist mit unserer IT-Tochter – und wer haftet?“

Paradigmenwechsel: von der Anlage zur Einrichtung

§ 30 Abs. 1 BSIG erfasst alle IT-Systeme, die der Dienstleistung dienen



Folge für Cloudingen: Die saubere Trennung von Netzleitstelle und Büro-IT bleibt technisch richtig – sie begrenzt den NIS-2-Pflichtenkreis der Stadtwerke AG aber nicht mehr.

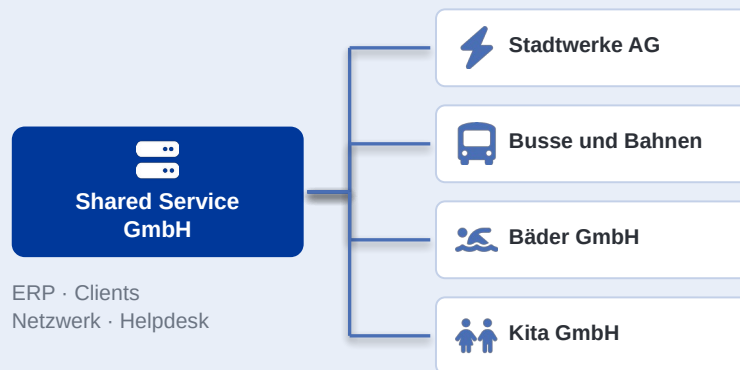
* OT = Operational Technology (Prozessleittechnik, hier die Netzleitstelle) · ERP = Enterprise Resource Planning · HR = Human Resources

Die Shared Service GmbH als Managed Service Provider

§ 2 Nr. 26 BSIG setzt Art. 6 Nr. 39 NIS-2-RL um – wer erbringt den Service?

Fall 1

Service bei der Tochter



MSP – aber Rückausnahme § 28 Abs. 4 S. 2 BSIG greift

Fall 2

Service bei der Holding

Holding wird selbst MSP – Sektor „Verwaltung von IKT-Diensten (B2B)“



Privilegierung des § 28 Abs. 4 S. 2 BSIG greift nicht mehr



Kennzahlen der Beteiligungen werden voll bzw. anteilig zugerechnet



bwE mit vollem Pflichtenkatalog – §§ 30, 32, 38 BSIG

Aber: Betreiberin einer kritischen Anlage wird sie nur, wenn sie deren Systeme selbst betreibt (§ 2 Nr. 22 BSIG).

Der Unterschied: Der MSP-Begriff ist in beiden Fällen erfüllt – konzernintern genügt, Eigentum an den Systemen ist nicht nötig. Über die Hochstufung entscheidet allein, wer die IT steuert: der Vertrag oder die Mutter.

* MSP = Managed Service Provider (Anlage 1 Nr. 6.1.10 BSIG) · MSSP = Managed Security Service Provider (Nr. 6.1.11) · IKT = Informations- und Kommunikationstechnik · bwE = besonders wichtige Einrichtung

Governance und Verträge: § 38 BSIG und Flow-down

Wer entscheidet – und was in jedem Outsourcing-Vertrag stehen muss

Wer trägt die Verantwortung?

Gesellschafterversammlung

Kommune als Gesellschafterin



Aufsichtsgremien

Überwachung der Töchter



Geschäftsleitung

Risikomanagementmaßnahmen umsetzen ·
Umsetzung überwachen · schulen

§ 38 BSIG

Was heißt „umsetzen“? Auslegung „lost in translation“?

DE
billigen

EN
approve

ES
aprobar

FR
approuver

Flow-down entlang der Lieferkette

Stadtwerke AG



Shared Service
GmbH



Lieferanten



Auditrechte

beim Dienstleister und dessen Lieferanten



Meldewege

Sicherheitsvorfälle binnen 24 Stunden



Patchmanagement

Fristen, Zuständigkeit, Nachweis



Backup & Recovery

Testpflichten und Wiederanlaufzeiten

Deutscher Sonderweg? Deutsche Fassung der NIS-2 Richtlinie bestimmt in Art 20: „ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit **billigen**, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können.“

Im **BSIG** wird von „umsetzen“ und „überwachen“ gesprochen. → Reicht das reine „Delegieren“ der Aufgabe zum Umsetzen? **NEIN**. Es geht um Verantwortung. Verantwortung kann die Geschäftsleitung nicht delegieren. Alle drei Vergleichsfassungen der NIS2-Richtlinie meinen eine förmliche Genehmigung – die deutsche ist schlicht schwach übersetzt. Auslegung im Sinne des „effet utile“. Der Streit um § 38 BSIG ist damit eher ein akademischer.

04

Prüfschema & Fazit

„Wie gehen wir jetzt konkret vor?“



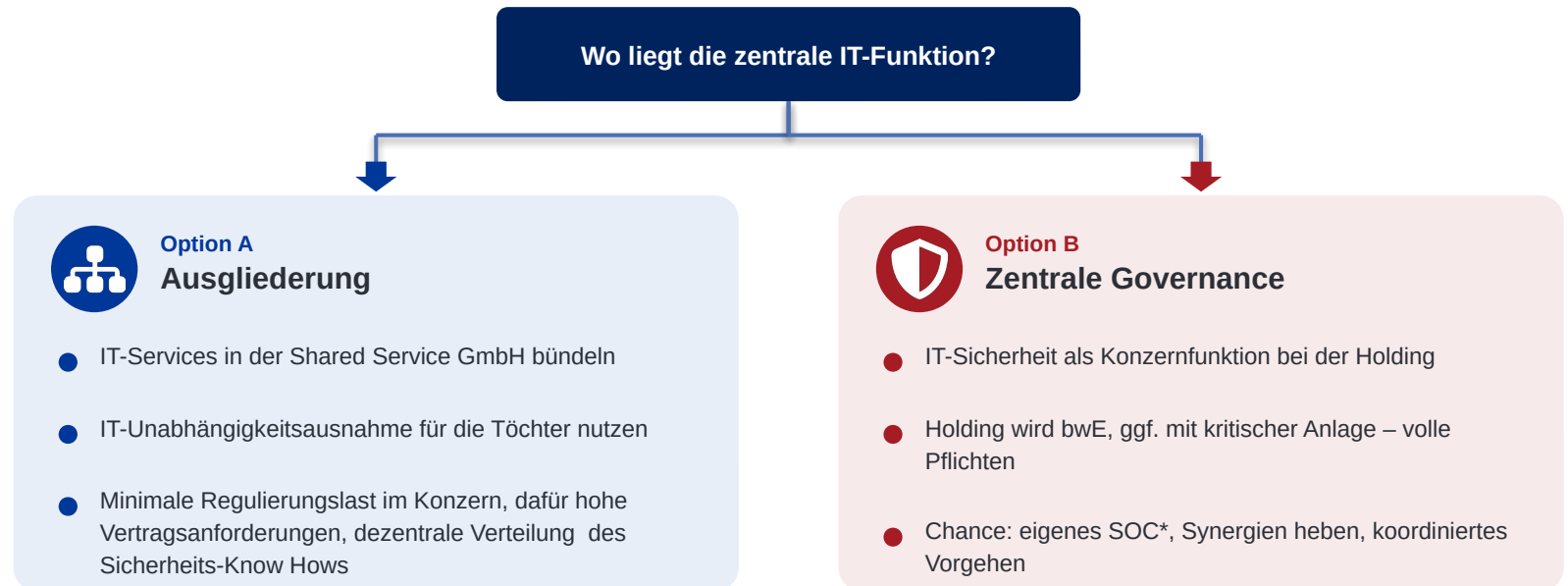
Das Prüfschema in vier Schritten

Auf jede Gesellschaft des Verbunds einzeln anzuwenden



Fazit: zwei Weichen für den kommunalen Konzern

Die Einstufung ist keine Formalie, sondern eine Strukturentscheidung



„Der Schutz der Freiheit entscheidet sich auch auf dem Schlachtfeld der IT-Sicherheit.“

* SOC = Security Operations Center · bwE = besonders wichtige Einrichtung

Vielen Dank.

Wir freuen uns auf Ihre Fragen und Anmerkungen.

Kristian Borkert · Gianna Nobile

Kristian.Borkert@juribo.de · Gianna.Nobile@juribo.de
www.juribo.de



JURIBO
LEGAL & CONSULTING