OpenKRITIS

NIS2 verspätet sich – und nun?

Februar 2025

Roadmap Regulierung

Nationale Umsetzung von NIS2 und RCE

bis 10/2024

ab 2025
~~ab 10/2024~~

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

EU RCE → Umsetzung durch → KRITIS-DachG

- Fokus: Physische Sicherheit und Resilienz
- Betroffen: KRITIS-Betreiber (kritische Anlagen)
- Schutzobjekt: Kritische Anlagen in DE und EU
- Deutsche Aufsicht (BBK)

bis 10/2024

ab 2025
~~ab 10/2024~~

Bundesamt für Sicherheit in der Informationstechnik

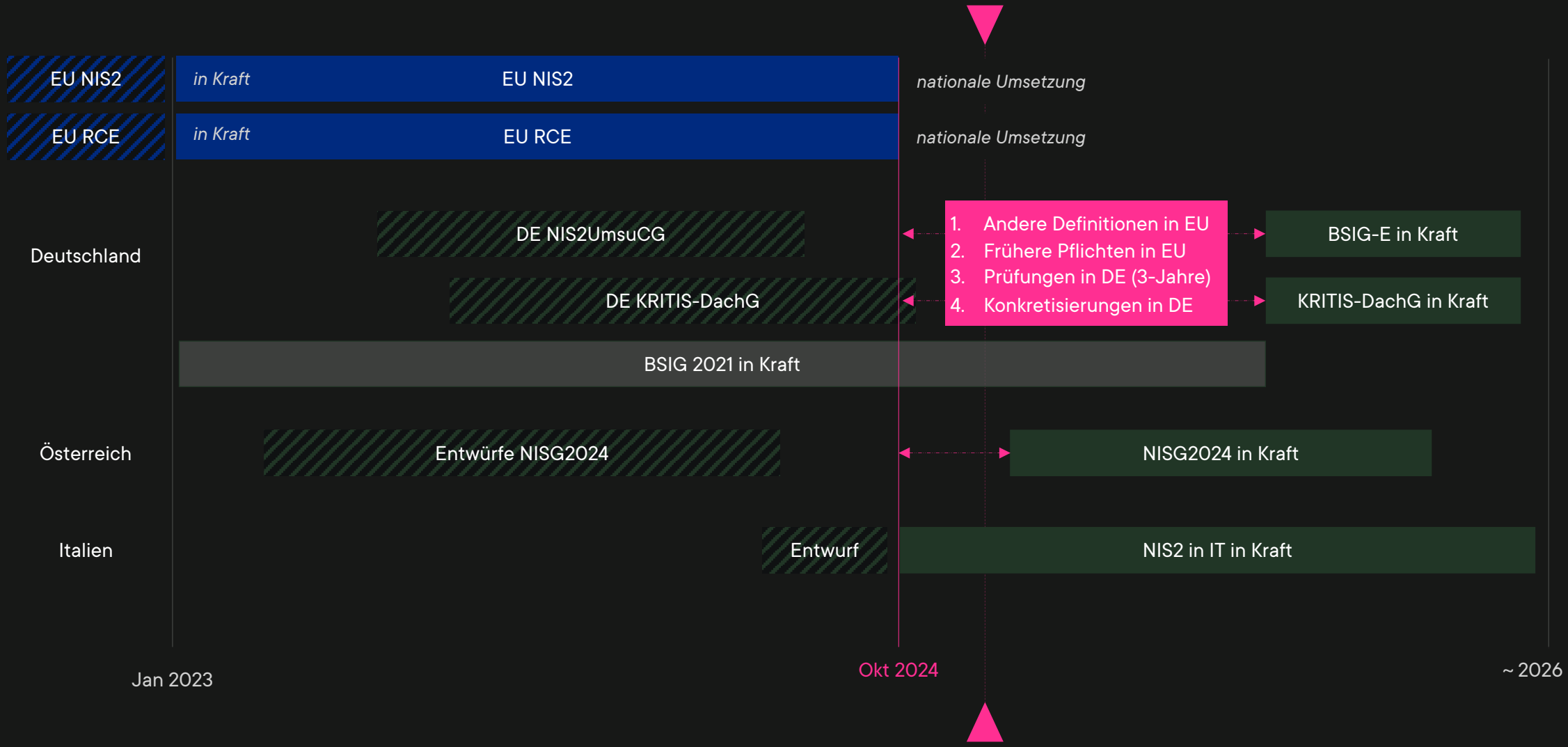
EU NIS2 → Umsetzung durch → NIS2UmsuCG

- Fokus: Cybersecurity und Informationstechnik
- Betroffen: KRITIS-Betreiber + besonders wichtige Einrichtungen + wichtige Einrichtungen
- Schutzobjekt: Große Teile der Wirtschaft
- Deutsche Aufsicht (BSI) + EU

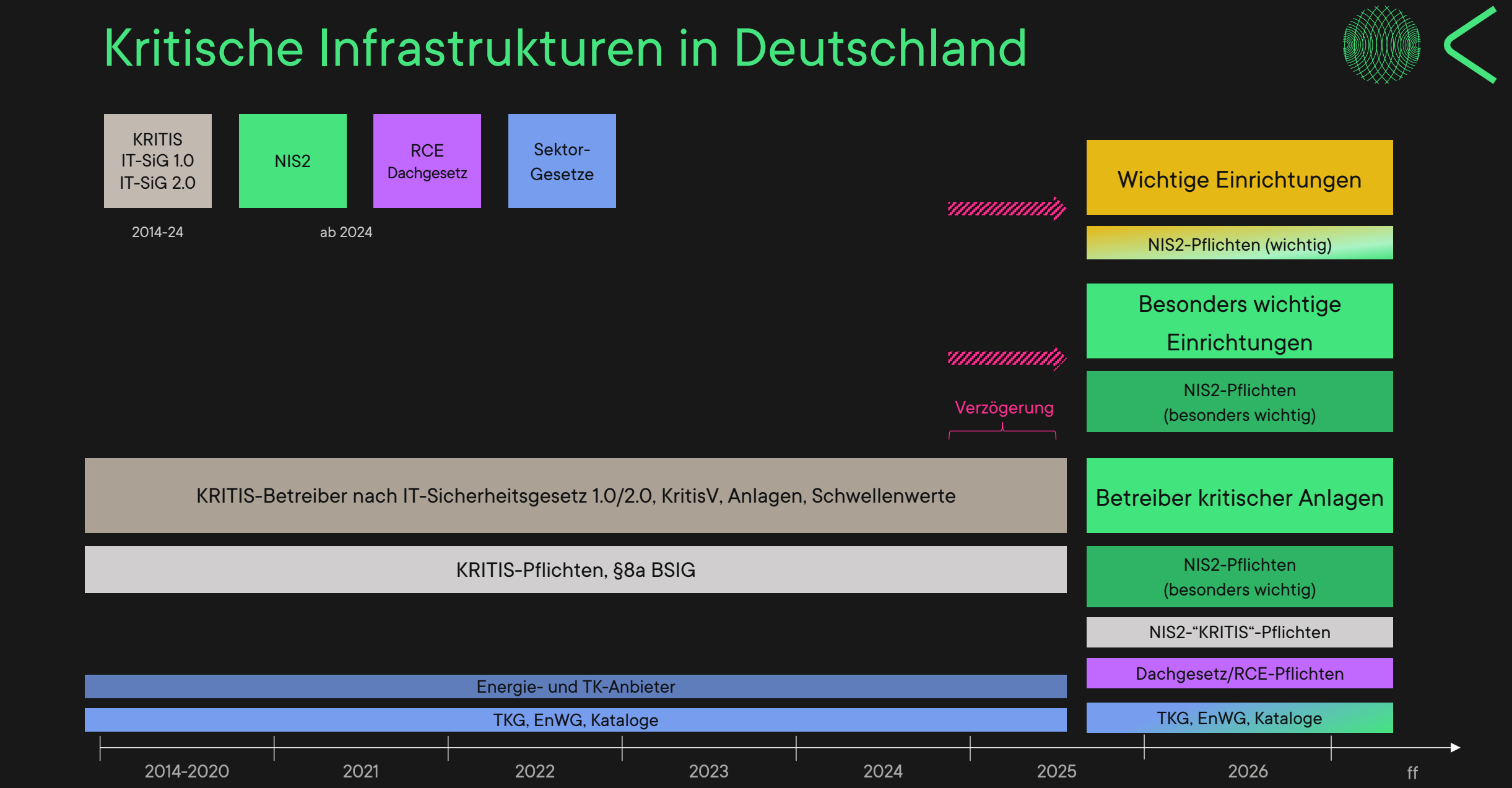
Verlauf Dachgesetz und NIS2

KRITIS-Dachgesetz		NIS2UmsuCG
	Apr 2023	Entwurf NIS2-Umsetzungsgesetz
Entwurf KRITIS-Dachgesetz	Jul 2023	Entwurf NIS2-Umsetzungsgesetz
	Sep 2023	Entwurf NIS2-Umsetzungsgesetz "Diskussionspapier"
	Okt 2023	Werkstattgespräch BMI und Verbände
Entwurf KRITIS-Dachgesetz	Dez 2023	Entwurf NIS2-Umsetzungsgesetz
Entwurf KRITIS-Dachgesetz	Mai 2024	Referentenenwurf NIS-Umsetzungsgesetz
	Jul 2024	Regierungsentwurf NIS2-Umsetzungsgesetz
Regierungsentwurf KRITIS-Dachgesetz	Nov 2024	div. Regierungsentwürfe, Formulierungshilfen
Inkrafttreten: Vermutlich 2025/2026?	2025	Inkrafttreten: Vermutlich H2 2025?

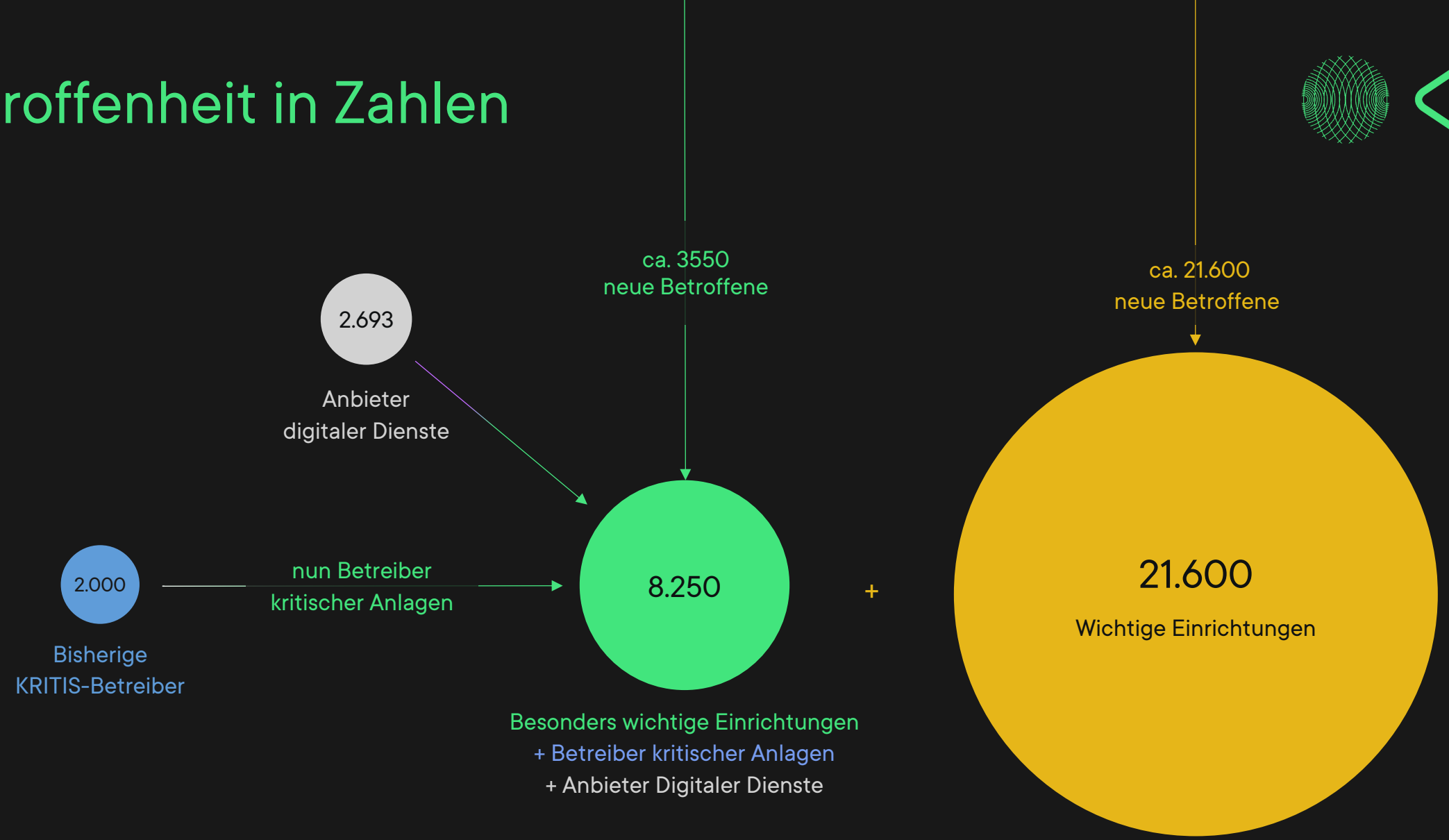
Sicht auf die EU



Kritische Infrastrukturen in Deutschland

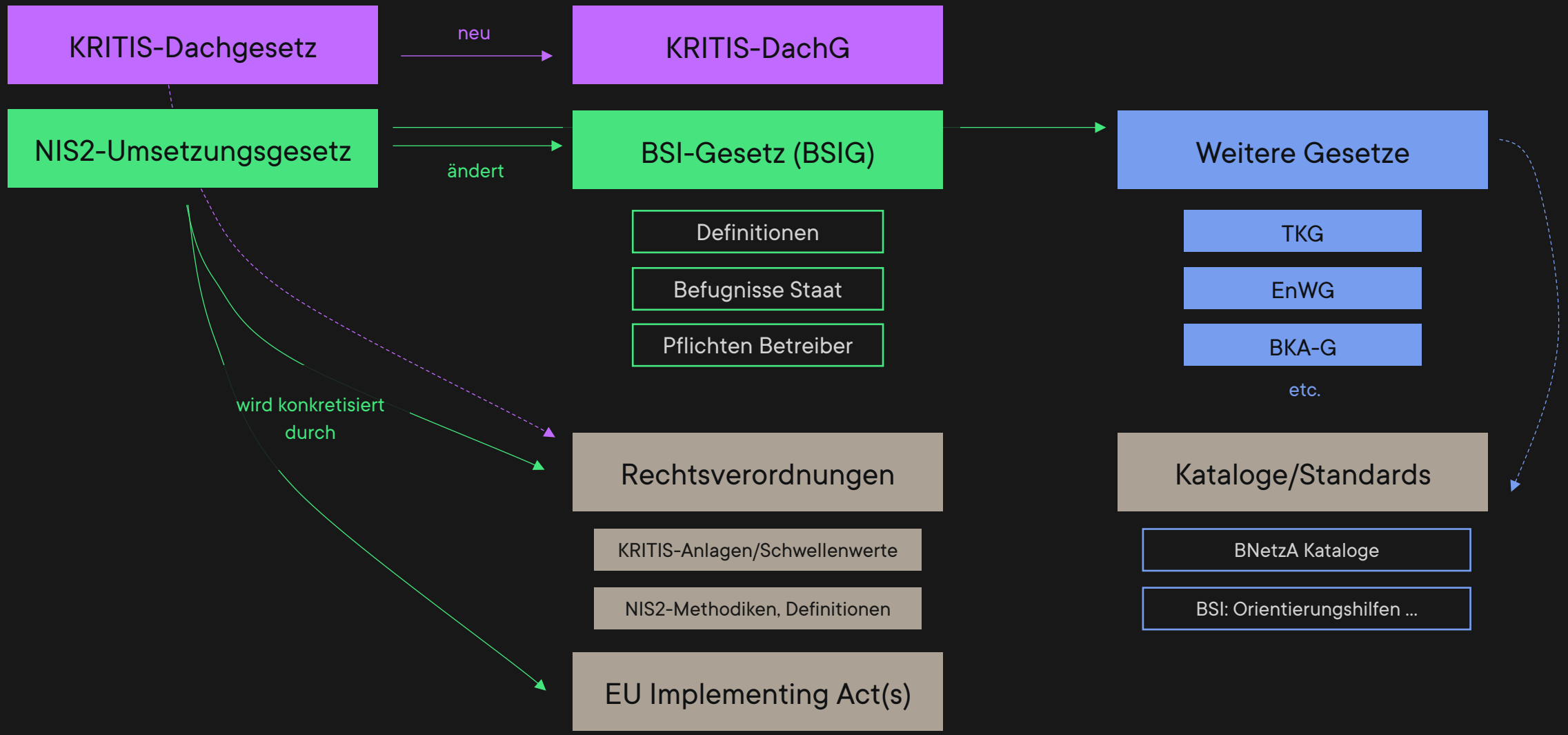


Betroffenheit in Zahlen



Erfahrung andere EU-Länder:
Deutlich mehr Unternehmen

Nationale Gesetze und Regulierung



Betroffenheit

Betreibergruppen und betroffene Sektoren

Betreiber kritischer Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen	
2.000	6.250	21.600	
Betreiber (KRITIS)	Großunternehmen + Sonderfälle	Mittlere Unternehmen	Großunternehmen Mittlere Unternehmen

mehrfach reguliert mit EnWG und TKG

EU

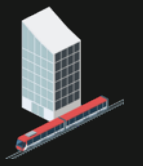
DORA

- Energie
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser
- Digitale Infrastruktur
- Siedlungsabfallentsorgung
- Weltraum
- Ernährung
- Bundeseinrichtungen

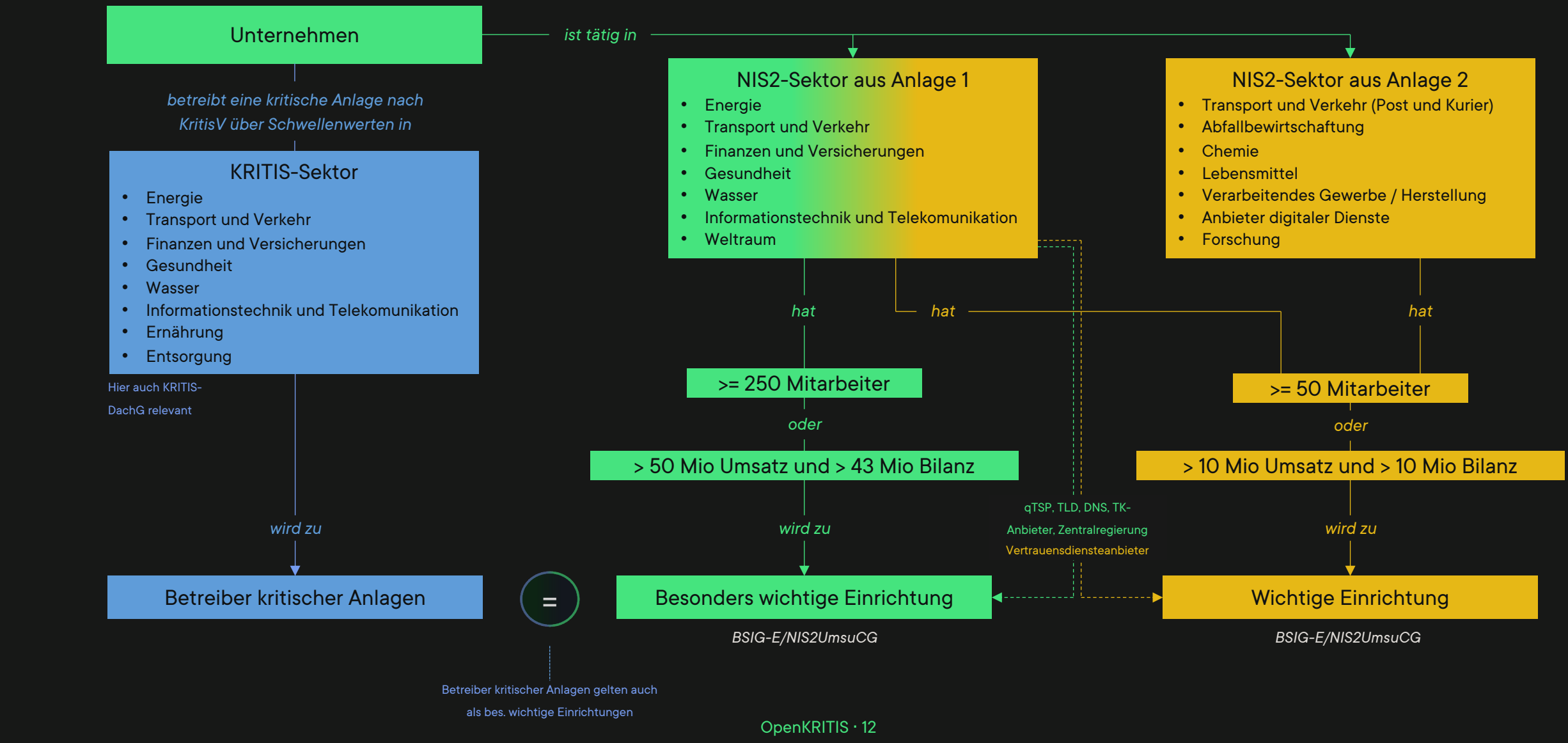
- Post und Kurier
- Chemische Stoffe
- Verarbeitendes Gewerbe
- Forschung
- Anbieter Digitaler Dienste
- Siedlungsabfallentsorgung
- Ernährung

Betreibergruppen und Schwellenwerte

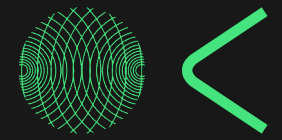
Unternehmen	Sektoren	Mitarbeiter	Umsatz	Bilanz
Besonders wichtige Einrichtungen	NIS2 Anlage 1	a) ≥ 250 b)	> 50 Mio. EUR und	> 43 Mio. EUR
Wichtige Einrichtungen	NIS2 Anlage 1 NIS2 Anlage 2	a) ≥ 50 b)	> 10 Mio. EUR und	> 10 Mio. EUR
Sonderfälle	NIS2 Anlage 1 NIS2 Anlage 2	größenunabhängig (DNS, TSP, TK ...)		
Kritische Anlagen	KRITIS-Sektoren	Schwellenwerte werden pro Anlage definiert		
Energie und TK-Anlagen und Netze	TKG und EnWG	Nach Diensten/Leistung/Nutzern definiert		



Betroffenheitsanalyse für NIS2



Von der Identifikation zu den Nachweisen



Wichtige Einrichtungen

> Unternehmensgröße

Besonders wichtige Einrichtungen

> Unternehmensgröße

Betreiber kritischer Anlagen

> Schwellenwerte Anlage

3 Monate

3 Monate

Registrierung beim BSI

Informationen an das BSI

BSI/BBK bestimmt initiale Nachweisfrist

Maßnahmen umsetzen § 30 NIS2

§§ 30, 31 NIS2 und Dachgesetz

Dokumentationspflicht

alle 3 Jahre

Nachweise an das BSI

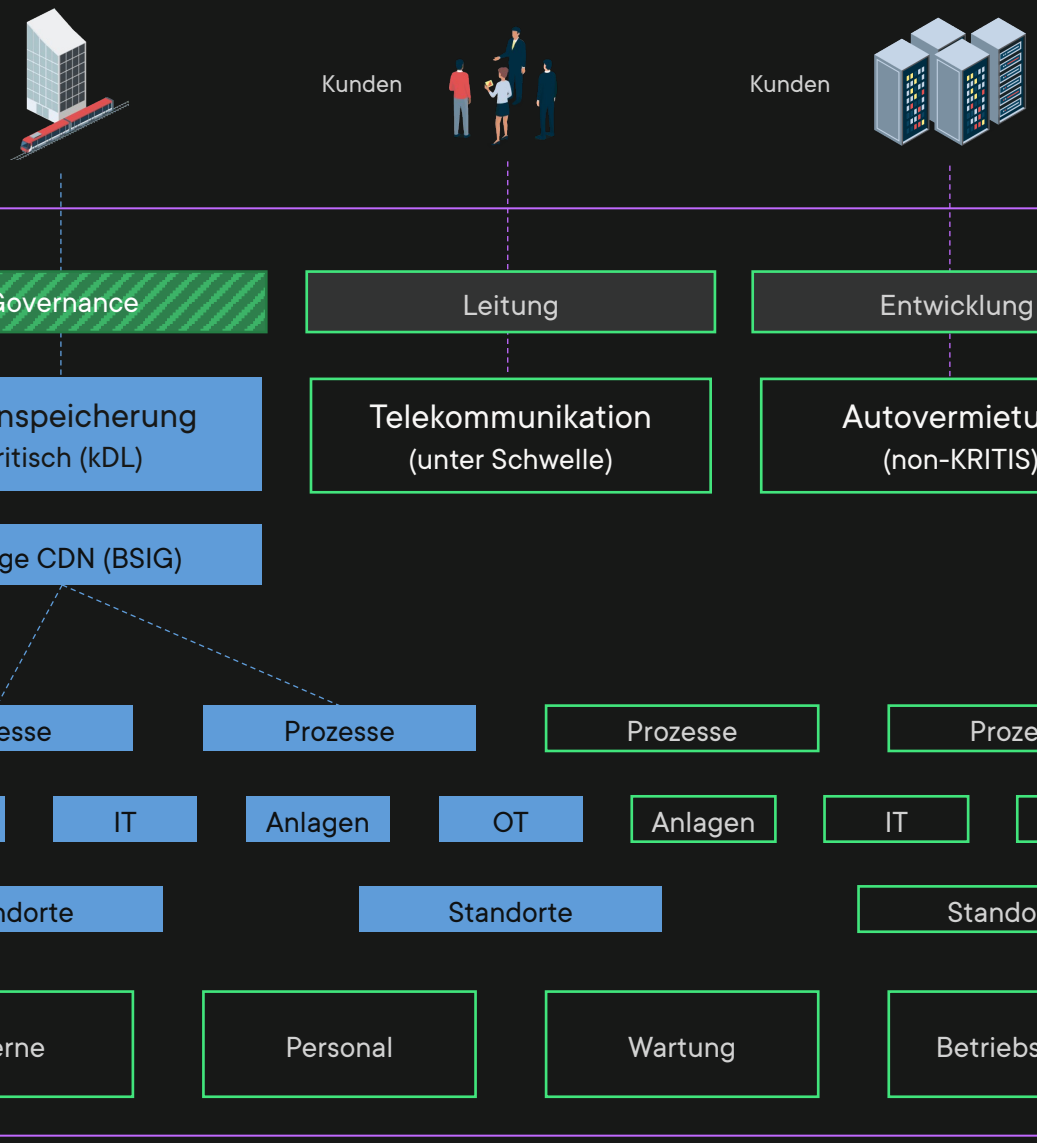
Prüfungen nach Anlass

Prüfungen nach Stichprobe

Audits, Prüfungen oder Zertifizierungen

NIS2-Maßnahmen, SzA, Dachgesetz

KRITIS-Geltungsbereich (alt)



KRITIS-Anlage (BSIG 2021)

- §8a BSIG (Sicherheit)
- Risiko-Management und Maßnahmen
- Meldepflichten, Registrierung, Prüfung

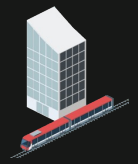
Weiterer Betrieb (non-KRITIS)

- ISMS und Maßnahmen nach Bedarf
- Schnittstellen

Vielleicht im KRITIS-Scope

- Verantwortung anteilig

NIS2 und KRITIS ab 2025



Allgemeinheit
>500. Tsd Bürger

Kunden

Kunden

IT-Konzern

Governance | Leitung | Entwicklung

Datenspeicherung
kritisch (kDL)

Telekommunikation
(NIS2-Service)

Autovermietung
(non-NIS2)

Anlage CDN (BSIG)

Prozesse | Prozesse | Prozesse | Prozesse

Anlagen | IT | Anlagen | OT | Anlagen | IT | OT

Standorte | Standorte | Standorte

Externe | Personal | Wartung | Betriebsmittel

Kritische Anlage (BSIG-E NIS2)

- §30/31/39 BSIG-E (Sicherheit)
- Risiko-Management und Maßnahmen
- Meldepflichten, Registrierung, Prüfung
- EU NIS2 Implementing Act

Einrichtung IT (NIS2)

- §30 Risiko-Management und Maßnahmen
- EU NIS2 Implementing Act

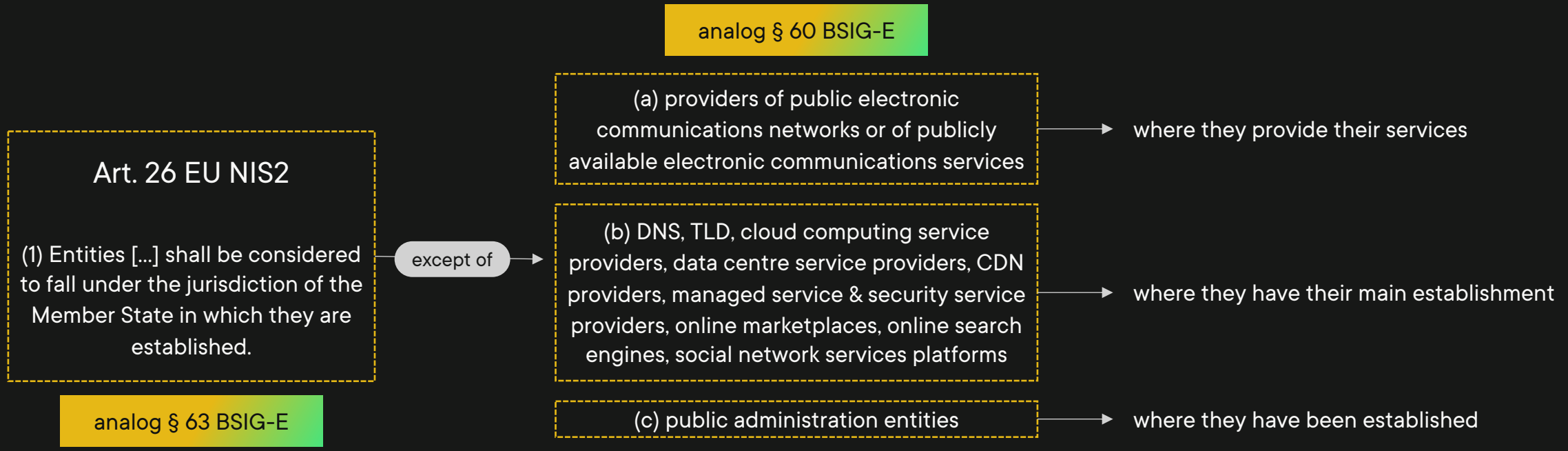
Einrichtung Telekommunikation (NIS2)

- §165 TKG-E
- Meldepflichten, Informationen, Registrierung

Autovermietung (non-NIS2)

- Risiko-Management und Maßnahmen
- Meldepflichten, Informationen, Registrierung,

Zentrale Zuständigkeit in der EU



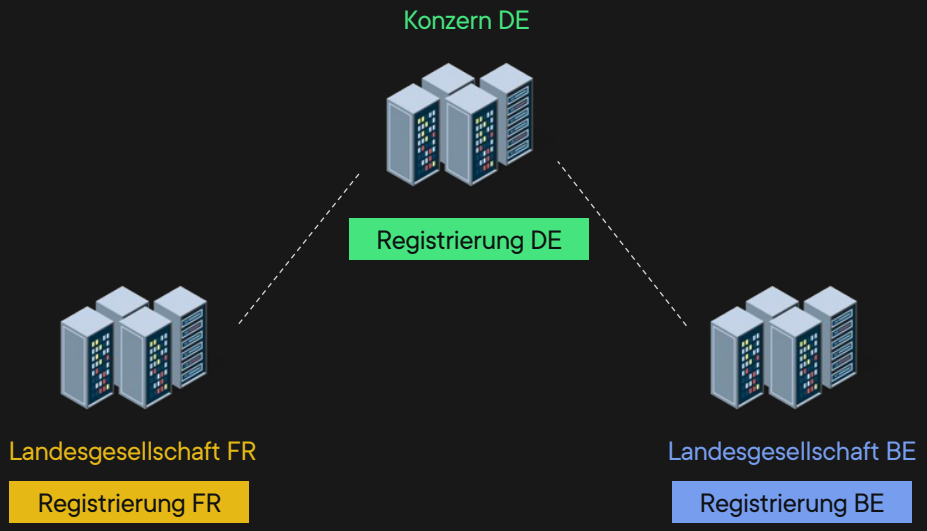
2. For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

3. If an entity [...] is not established in the Union, but offers services within the Union, it shall designate a representative in the Union [...]

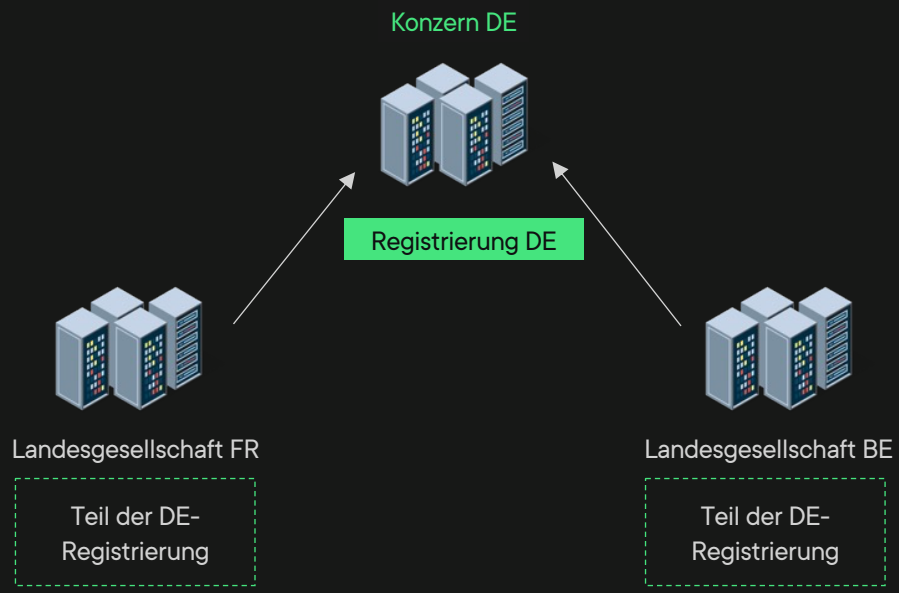
EU NIS2-Direktive, Artikel 26 Nr. 2, 3

Zentrale Zuständigkeit: Beispiele

NIS2-Einrichtung



Managed Services (IT)



Dienstleister-Pflichten durch Erwartungen

Betreiber
KRITIS/NIS2

erwartet

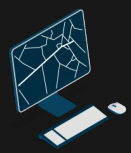
Dienstleister

„KRITIS/NIS2 Compliance“

- Incident reporting
- Tests
- Audits
- Nachweise
- Sichere IT
- Standards

Erwartungen häufig in existierenden Verträgen und SLAs

„muss sicher betrieben werden“ == NIS2



?

In Produkten

Pflichten im Vertragsmanagement

Betreiber
KRITIS/NIS2

alle DL

Verträge

Vertragsmanagement notwendig!

„KRITIS“
or NIS2
Spezifika

- Service-Beschreibung
- Management vom Vertrag
- Sicherheitsanforderungen
- Zertifizierungen (ISO 27001, QM, ...)
- Zusammenarbeit bei Meldungen
- Zusammenarbeit für Behörden
- Awareness, Schulungen

Generische Mindest-anforderungen an Provider Management

- Spezifische Sicherheitsanforderung
- Sichere Entwicklung
- Meldefristen
- Produkte/Komponenten (CC, EU)
- KRITIS, Sektorspezifika
- Test und Analyse

Spezifische Anforderungen für NIS2/KRITIS-Bereiche, Funktionen etc.

Cybersecurity-Pflichten

Pflichten für Unternehmen in DE NIS2 (BSIG-E)

Risikomanagement

Meldepflichten

Registrierung

Nachweise

Informationspflichten

Governance

KRITIS-Anforderungen

! Diverse Ausschlüsse und Sonderregeln für Maßnahmen und Vorgaben: Teils durch Sektorgesetze, BNetzA, teils durch EU-Vorgaben reguliert: Telekommunikation, Cloud/Online/Provider, Energieversorgung, nationale Sicherheit.

- Einrichtungen
- Kritische Anlagen
- EU-Vorgaben (IA)
- Sektor-Ausnahmen

Pflichten für Unternehmen in NIS2 BSIG-E

§ 30

Risikomanagement

- ISMS, IT-RM, Risiko-analysen, Allgefahren
- Incident Management
- Business Continuity
- Supply Chain, Zulieferer
- Training
- MFA und SSO
- Zugangskontrolle
- Notfall-Kommunikation
- Zertifizierte Produkte

§ 32

Meldepflichten

- BSI: zentrale Meldestelle
- 24h/72h/30 Tage
- Inhaltliche Vorgaben
- Zwischenmeldungen
- (~ CERT/SOC/SIEM)

§§ 33, 34

Registrierung

- Eigenständige Identifikation und Registrierung
- Frist: 3 Monate
- Registrierung auch durch BSI möglich
- Bestimmte Einrichtungen müssen sich bis 17.01.25 registrieren

§ 39

Nachweise

Betreiber kritischer Anlagen:

- Prüfungen/Audits analog der KRITIS-Prüfungen
- Inklusive OH SzA
- Alle drei Jahre

Alle Einrichtungen:

- Stichproben durch BSI
- Dokumentationspflicht
- Mögliche Einsichtnahme

Pflichten für Unternehmen in NIS2 BSIG-E

§ 35

Informationspflichten

- BSI: Weisungsbefugnis für Unterrichtung von Kunden über Sicherheitsvorfälle
- Spezielle Sektoren: Abhilfemaßnahmen
- BSI operative Beratung bei Frühwarnung
- BSI: Weisungsbefugnis für Veröffentlichung Sicherheitsvorfall

§ 38

Governance

- Geschäftsleiter müssen Risikomanagement-maßnahmen umsetzen
- Geschäftsleiter haften für Schaden bei Pflicht-verletzung §38
- Pflicht-Schulungen

§ 31

KRITIS-Anforderungen

- Angriffserkennung zus. verpflichtend OH SzA
- Kontinuierlicher Einsatz im Betrieb
- Komplexe Infrastruktur
- Nachweispflicht
- BSI darf überprüfen
- Besondere Sorgfalt bei Auswahl Maßnahmen

§ 61

Sanktionen

- Neue Tatbestände
- Bestehende Bußgelder teils deutlich erhöht
- Geschäftsführer haften
- Allg. Tatbestände
- Wichtige Einrichtungen
- Besonders wichtige Einrichtungen
- Betreiber kritischer Anlagen

Pflichten für Unternehmen im KRITIS-Dachgesetz

§ 8

Registrierung

- Frist: 3 Monate
- Kontaktstelle einrichten
- BBK darf eigenständig registrieren

§ 12

Risikoanalyse

- Frist: alle 4 Jahre
- Naturkatastrophen, sektorübergreifende Risiken, feindliche Bedrohungen, Wirtschaftsstabilität
- Sektorspezifische Ausnahmen
- Vorlagen durch BBK möglich

§ 13

Resilienz maßnahmen

- Frist: 10 Monate
- Physischer Schutz
- Reaktion, Abwehr, Folgenbegrenzung
- Wiederherstellung
- Schulungen, Übungen
- Konkrete Maßnahmen: §13 (3)
- Darstellung in Resilienzplan
- Branchenspezifische Resilienzstandards

§ 18

Meldepflicht

- Frist: 10 Monate
- Vorfallsmeldungen für erhebliche Störungen
- Kontaktstelle: BBK / BSI
- Frist: 24h / 1 Monat
- Inhaltliche Vorgaben
- Ausgestaltung Meldeverfahren durch BBK möglich

§ 16

Nachweise

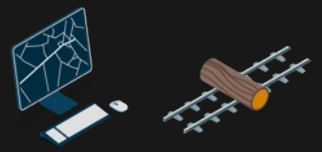
- Nachweise auf Nachfrage der Aufsichtsbehörde
- darf bei Zweifeln nachprüfen
- Audits (wie KRITIS)
- BBK macht Vorgaben zu Audit-Durchführung

§ 24

Sanktionen

- Höhe bis 1 Mio. EUR
- 11 Tatbestände bei Vorsatz Ordnungs-widrigkeiten
- Verspätete Registrierung
- Keine Risikoanalysen
- Unzureichende Resilienzmaßnahmen
- ...

Meldewesen für Betreiber kritischer Anlagen



Erheblicher Sicherheitsvorfall

Interne Meldestelle

< 24 Std.

- Verdacht rechtswidrige Handlungen
- Grenzüberschreitende Auswirkungen
- Art der betroffenen Anlage, kDL, Auswirkungen auf kDL
- Anzahl und Anteil betroffene Nutzer
- Bisherige und voraussichtliche Dauer
- Geografisches Gebiet
- Informationen Beurteilung Art, Ursache, Folgen

72 Std.

- Bestätigung / Aktualisierung Erstmeldung
- Erste Bewertung mit Schweregrad, Auswirkungen, Kompromittierungs-indikatoren

Zwischen-meldungen

- Auf Ersuchen des BSI
- Relevante Statusaktualisierungen

1 Monat

- Ausführliche Beschreibung mit Schweregrad, Auswirkungen
- Art der Bedrohung / Ursache
- Abhilfemaßnahmen
- Ggf. grenzüberschreitende Auswirkungen
- „ausführlicher Bericht“

Meldestelle von BBK und BSI

- Vorgaben aus NIS2UmsuCG
- Vorgaben aus KRITIS-Dachgesetz

EU Implementing Acts

Europäische Kommission

KANN → **Risikomanagement**
Art. 21 (5) UAbs 2 EU NIS2

- Konkretisierung für Cybersecurity-Maßnahmen (DE: § 30 BSIG-E)
- Technische, methodische Anforderungen, ggf. auf Basis ENISA

MUSS → **Internet und Digitales**
Art. 21 (5) UAbs 1 EU NIS2

- Konkretisierung für Cybersecurity-Maßnahmen für bestimmte Internet-Provider (DE: § 30 BSIG-E)
- Technische, methodische und sektorspezifische Anforderungen
- Geltungsbereich: DNS-Provider, TLDs, Cloud Computing Provider, CDNs, Rechenzentrums-Dienste, Managed (Security) Services Provider, Online-Marktplätze, Suchmaschinen, soziale Netzwerke

MUSS → **Meldepflichten**
Art. 23 (11) UAbs 2 EU NIS2

- Konkretisierung für Meldepflichten und zur Einstufung als „erheblich“
- Soll mindestens für o.g. Internet-Provider gelten
- Geltungsbereich kann erweitert werden

Implementing Acts haben Vorrang vor nationalen Regelungen, auch vor Rechtsverordnung nach § 2 (2) BSIG-E

NIS2-Pflichten und Implementing Act

BSIG-E Juli 2024	Anforderung
Risikomanagement §30 (1)	Einrichtungen sind verpflichtet …
Maßnahmen §30 (2)	Konzepte Risikoanalyse und Sicherheit in der IT
	Bewältigung von Sicherheitsvorfällen
	Aufrechterhaltung des Betriebs und Krisenmanagement
	Sicherheit der Lieferkette
	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT
	Konzepte und Verfahren zur Bewertung der Wirksamkeit
	Cyberhygiene und Schulungen im Bereich der Sicherheit
	Kryptografie und Verschlüsselung
	Sicherheit des Personals, Zugriffskontrolle und Asset Management
	Multi-Faktor-Authentifizierung oder SSO, gesicherte Sprach-, Video- und Textkommunikation, Notfallkommunikationssysteme
§31, §33, §39	KRITIS, SzA, Registrierung, Nachweise, Informationen …
§32	Meldepflichten, Vorfallsmeldungen

Implementing Act
Verpflichtend für IT-Provider

Erweitert NIS2
Erweiterung der Punkte aus Artikel RL (und §30)

>150 Kontrollen
Viele detaillierte Anforderungen

Mapping ISO 27001
Gute Abdeckung (80%) in 27002

Beispiel Implementing Act

4.3. Crisis management

4.3.1. The relevant entities shall put in place processes for crisis management.

4.3.2. The relevant entities shall ensure that crisis management processes address at least the following elements:

(a) roles and responsibilities for personnel, ensuring that all staff know their roles in crisis situations, including specific steps to follow;

(b) appropriate communication means between the relevant entities and relevant competent authorities;

(c) application of appropriate controls such as supporting systems, processes and additional capacity.

For the purpose of point (b), the flow of information between the relevant entities and relevant competent authorities shall include both obligatory communications, such as incident reports and related timelines, and non-obligatory communications.

4.3.3. The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or security controls.

4.3.4. The relevant entities shall test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks.

4
Business Continuity and Crisis Management

4.1 BC and DR plans

4.2 Backup management

4.3 Crisis management

Mapping NIS auf ISO 27001 und KRITIS

NIS2: Mapping auf KRITIS und ISO

Nr.	NIS2UmsuCG	Anforderung	KRITIS	ISO 27001
30.1.1	§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen	BSI-3 BSI-15	4.3 A.5.4 A.5.29 A.5.30
30.1.2	§30 (1) Satz 3	Dokumentation der NIS2 Risiko-Management Maßnahmen	BSI-16	6.1.3 8.3 A.5.31
30.2.0	§30 (2) Satz 1	Allgefahrenansatz und Stand der Technik	BSI-13 BSI-15	6.1 8.2 8.3 A.5.29 A.5.30
30.2.1a	§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	BSI-13 BSI-14	6.1 8.2 8.3
30.2.1b	§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	BSI-1 BSI-2	4.1-10.2 A.5.1 A.5.2 A.5.4

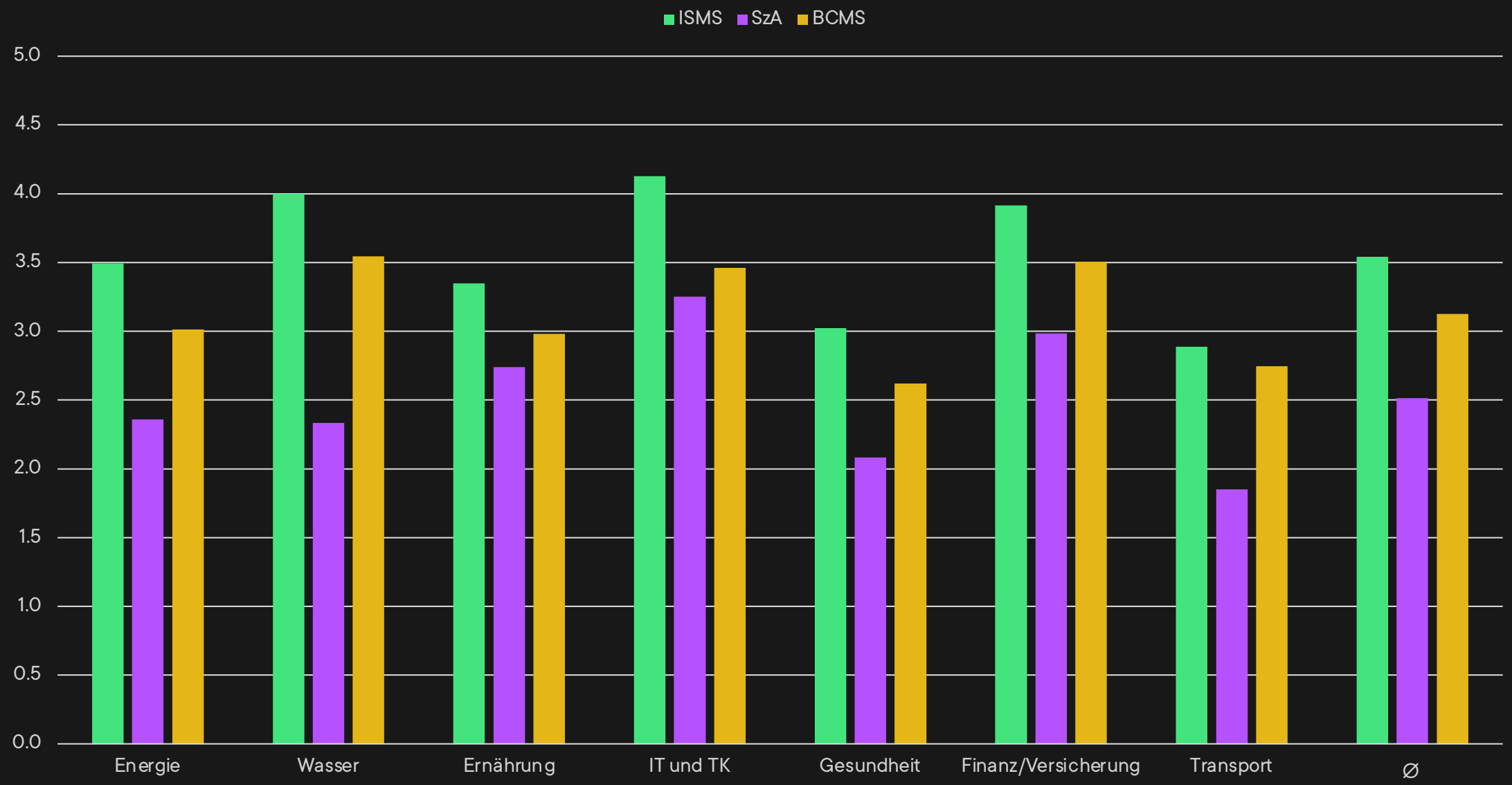
openkritis.de/massnahmen/nis2-mapping-standards-implementing.html

KRITIS (KdA): Mapping auf NIS2, ISO und RUN

KdA	Anforderung	C5 2020	NIS2 IT-Act	ISO 27001 2022	RUN Grad
BSI-1	Managementsystem für Informationssicherheit	OIS-01	1.1.1 7.1	4.1-10.2	1
BSI-2	Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung	OIS-02	1.1.1 1.1.2	6.2 A.5.1 A.5.2 A.5.4	2
BSI-3	Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit	OIS-03	1.2.1 1.2.2 1.2.4	4.3 A.5.3 A.5.4	2/3
BSI-4	Funktionstrennung	OIS-04	1.2.5	A.5.3	2
BSI-5	Asset Inventar	AM-01	12.4.1 12.4.2 12.4.3	A.5.9	3
BSI-6	Zuweisung von Asset Verantwortlichen	AM-02	-	A.5.4 A.5.10	2
BSI-7	Nutzungsanweisungen für Assets	AM-02	12.1.1 12.2.1	A.5.10 A.7.10	2

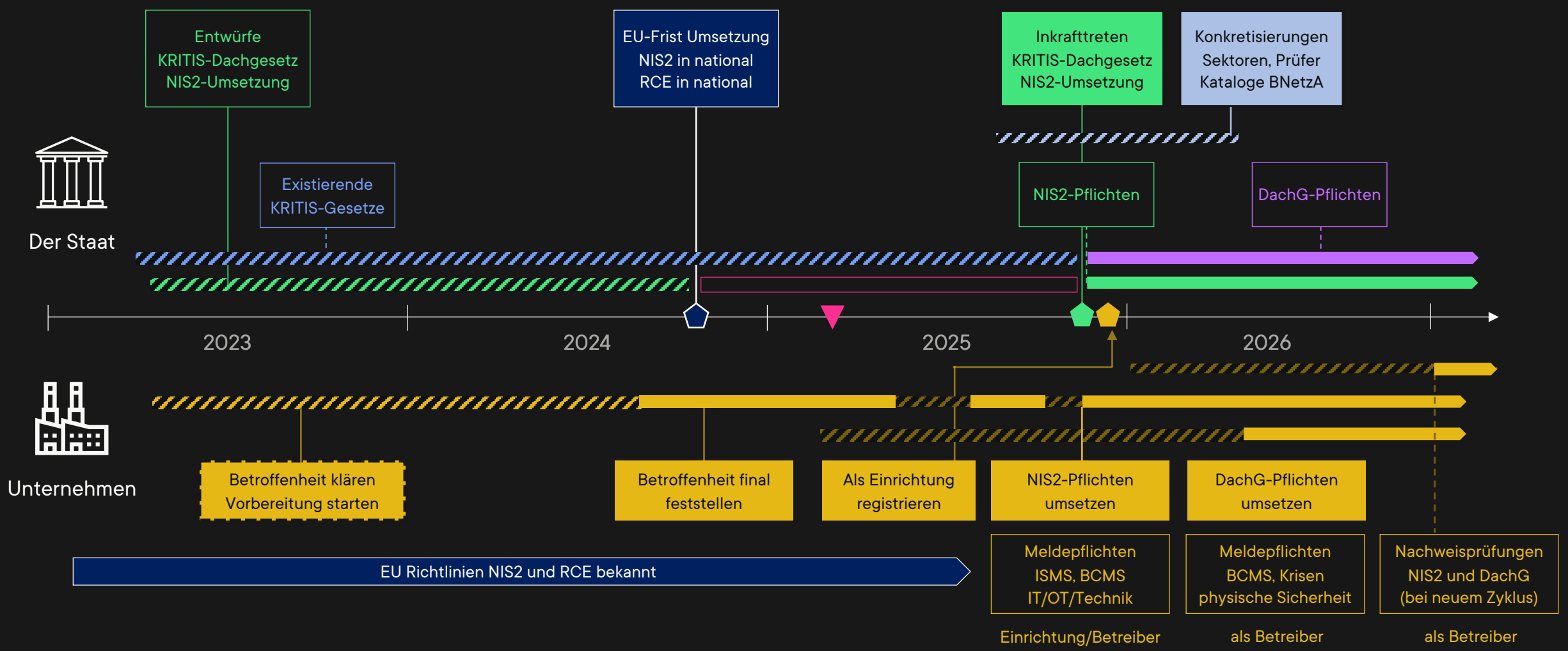
openkritis.de/massnahmen/kritis-mapping-standards.html

KRITIS in Zahlen
Quelle: BSI Aug 24



Und nun?

NIS2 und KRITIS ab 2025



NIS2-Programm und Verzögerung

EU-Frist NIS2

Neues DE Gesetz?

2023 | 2024 | 2025 | 2026

NIS2-Vorbereitung

EU NIS2 Richtlinie

DE NIS2 UmsuCG

Wartephase

Einrichtung

Vorbereitung Security-Maßnahmen

Vorbereitung Scoping

Vorbereitung Registrierung

Vorbereitung Meldefrist

Weiterarbeit an NIS2

EU NIS2 Richtlinie

NIS2-Umsetzung

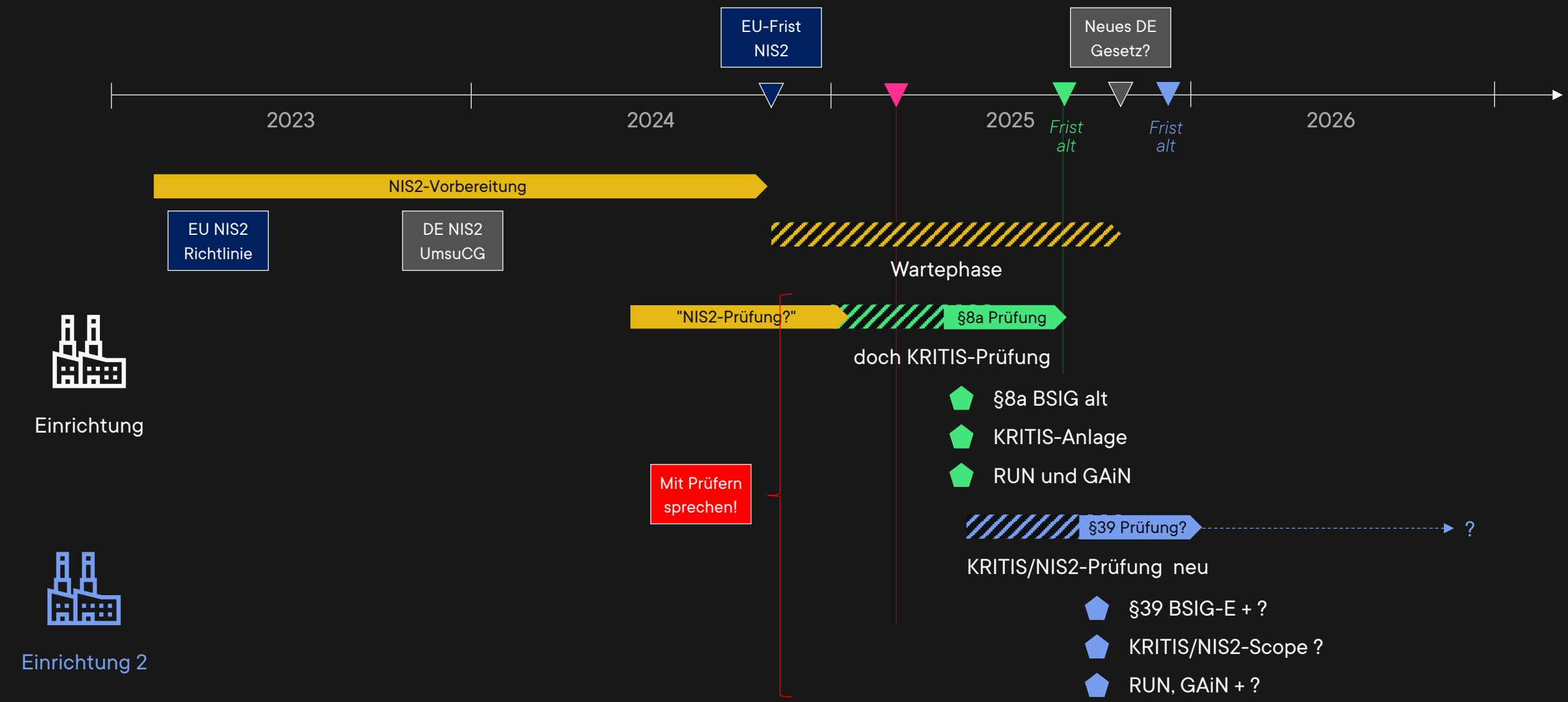
Anpassen

DE NIS2 UmsuCG

- Registrierung
- Meldefrist <24h
- §30 Maßnahmen
- Nachweise, Audit

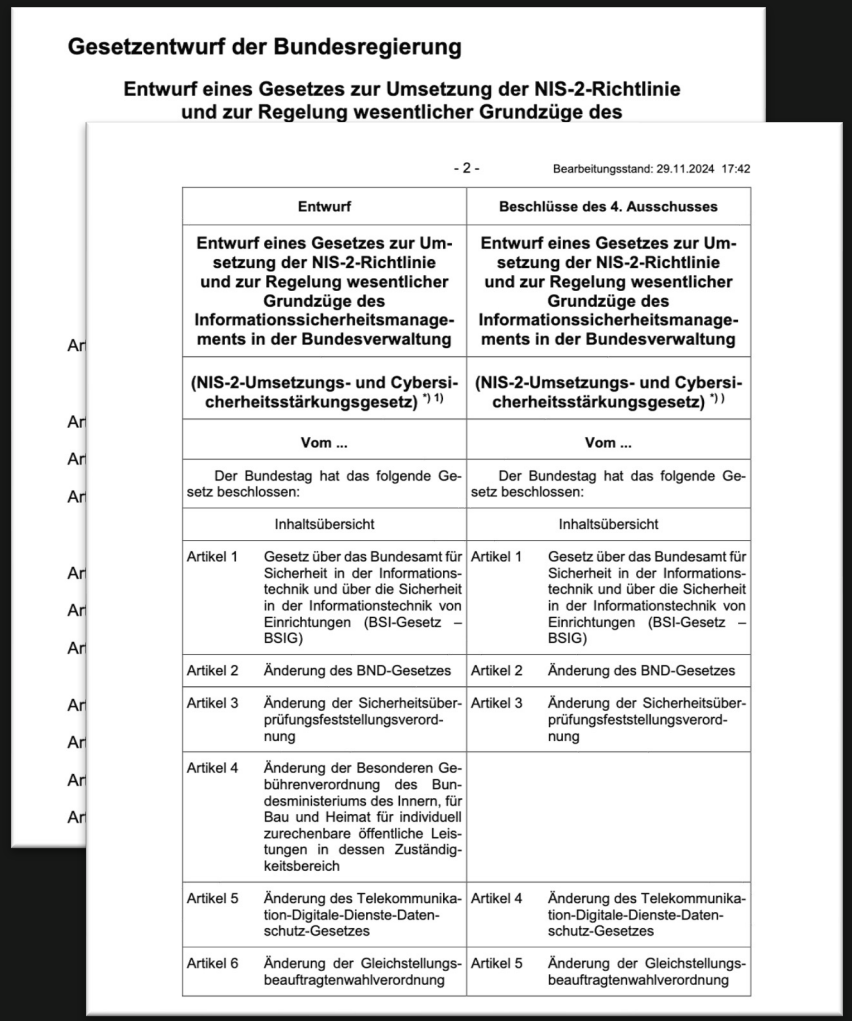
"Übergangsfrist"

KRITIS und verzögerte Prüfungen



Ausblick 2025

Entwürfe bis Q4 2024



Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des

- 2 - Bearbeitungsstand: 29.11.2024 17:42

Entwurf		Beschlüsse des 4. Ausschusses	
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung		**Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung**	
(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) *) 1)		**(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)** *)	
Vom ...		**Vom ...**	
Der Bundestag hat das folgende Gesetz beschlossen:		Der Bundestag hat das folgende Gesetz beschlossen:	
Inhaltsübersicht		Inhaltsübersicht	
Artikel 1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)	Artikel 1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)
Artikel 2	Änderung des BND-Gesetzes	Artikel 2	Änderung des BND-Gesetzes
Artikel 3	Änderung der Sicherheitsüberprüfungsfeststellungsverordnung	Artikel 3	Änderung der Sicherheitsüberprüfungsfeststellungsverordnung
Artikel 4	Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich		
Artikel 5	Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes	Artikel 4	Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes
Artikel 6	Änderung der Gleichstellungsbeauftragtenwahlverordnung	Artikel 5	Änderung der Gleichstellungsbeauftragtenwahlverordnung

NIS2UmsuCG 2025

Vermutungen 02/2025

Erst:

- Regierungsbildung
- Koalitionsvertrag und Agenda
- Ministeriumsverteilung

Aber:

- Vertragsverletzungsverfahren EU
- EU Richtlinie bekannt und eindeutig
- EU Richtlinie gibt Mindestrahmen vor

Vermutungen:

- Gesetz ähnlich wie letzte Entwürfe
- Viele DE-Anpassungen aus Q4 2024 = ?
- Grundsatz ist klar (EU RL), Timing TBD

Nichts zu Kritischen Infrastrukturen verpassen:

OpenKRITIS.de

KRITIS-Dachgesetz auf OpenKRITIS: KRITIS-Dachgesetz

NIS2-Umsetzung auf OpenKRITIS: NIS2 in Deutschland

Kontakt: info@openkritis.de und OpenKRITIS auf LinkedIn

NIS 2 und Mehrfachregulierung

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

EU NIS2 und KRITIS-Dachgesetz verspäten sich – und nun?
Stand: 13. Februar 2025
Version: 2.1

Impressum

Insignals GmbH
Paul Weissmann
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X

info@openkritis.de · +49 176 58952135