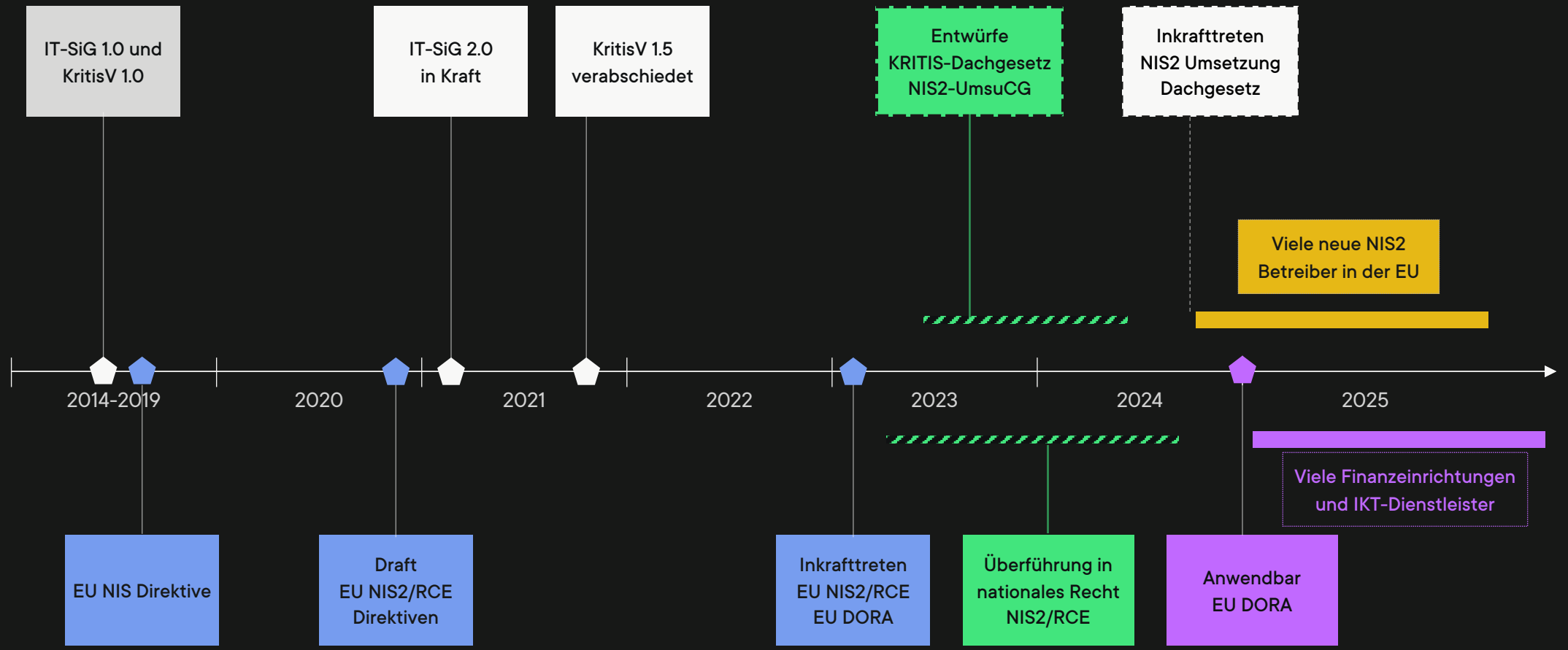
EU NIS2 Mehrfach-Regulierung

Mehr Regulierung in mehr Sektoren

Juli 2024

KRITIS in Deutschland seit 2014



Nationale Umsetzung von NIS2 und RCE

bis 10/2024

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

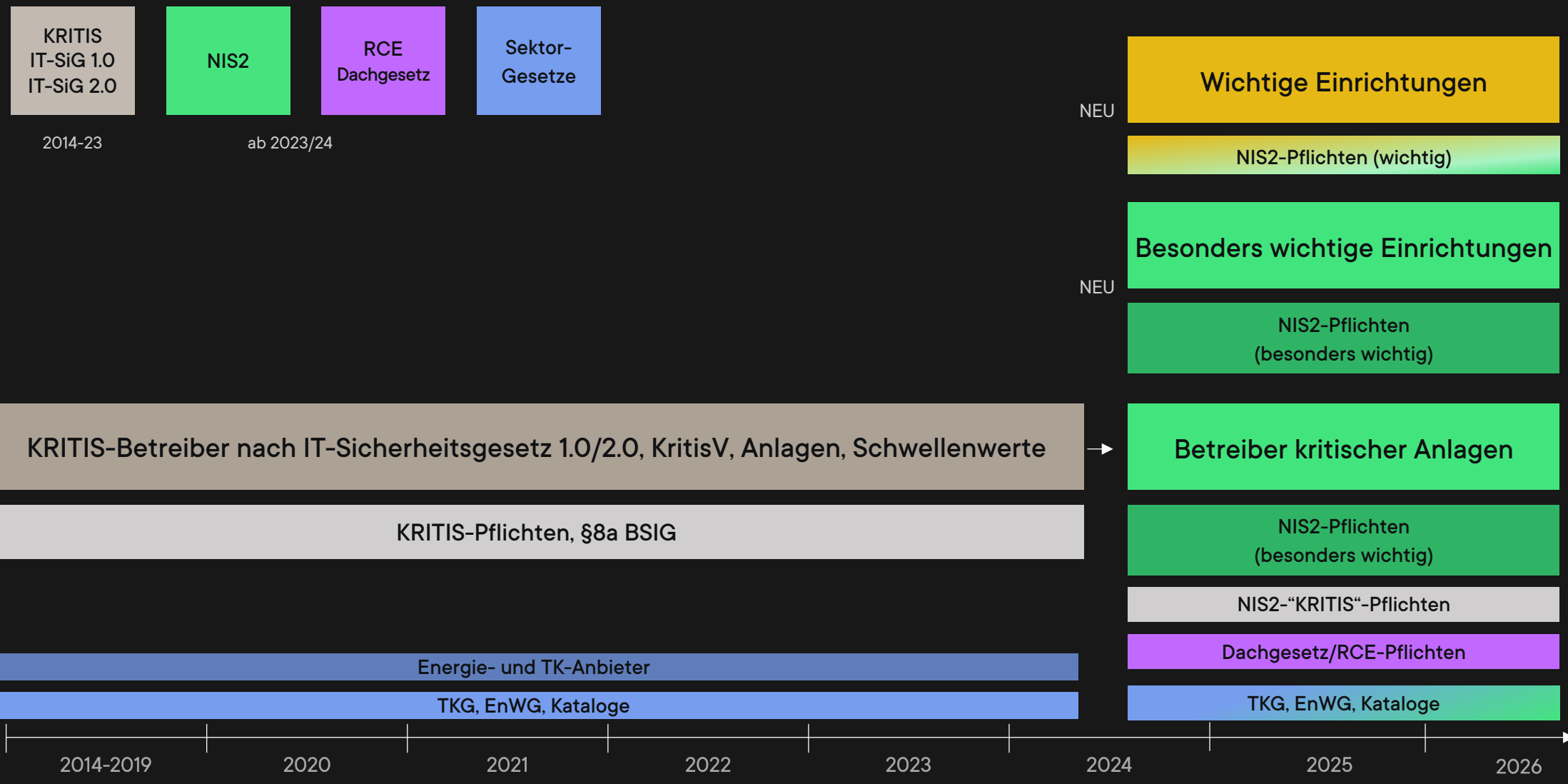
ab 10/2024

Bundesamt
für Sicherheit in der
Informationstechnik

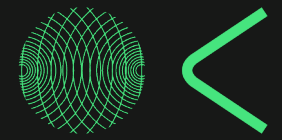
EU NIS2 → Umsetzung durch → NIS2UmsuCG

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

Kritische Infrastrukturen in Deutschland



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

- Energie
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser und Abwasser
- Digitale Infrastruktur

mehrfach reguliert mit EnWG und TKG

In großen Teilen von NIS2 ausgenommen

EU DORA

Teils auch als kritische IKT-DL

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

- Siedlungsabfallentsorgung
- Weltraum
- Ernährung
- Zentralregierung

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
Kritische Anlagen	KRITIS-Sektoren	Schwellenwerte werden pro Anlage definiert		
Energie und TK-Anlagen und Netze	TKG und EnWG	Nach Diensten/Leistung/Nutzern definiert		
Kritische IKT-Dienstleister	DORA	Finanzkunden & Festlegung durch ESA		

Einrichtungen und Betreiber im Sektor Energie

Einrichtungen

- Strom- & Gaslieferanten
- Stromerzeugungsanlagen
- Stromverteiler- & Übertragungsnetze
- Aggregatoren
- Wasserstoff
- Stromausgleich
- Erdöl-Fernleitungen
- Fernwärme- & -kälte
- Energie- & Gasspeicheranlagen
- Produktion, Raffination, Aufbereitung, Lagerung Erdöl
- Gasverteil- und Fernleitungsnetze
- Strommarktbetreiber
- Gewinnung, Raffination, Aufbereitung von Erdgas
- LNG

- Mind. 250 Mitarbeiter
- >50 Mio Umsatz + >43 Mio Bilanz

→ **Besonders wichtige Einrichtung**

- Mind. 50 Mitarbeiter
- >10 Mio Umsatz + Bilanz

→ **Wichtige Einrichtung**

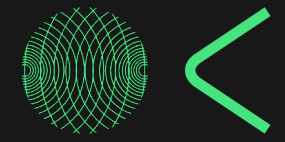
→ **Energieanlage oder Netz (EnWG) - separat**

Betreiber

- 5 Anlagen in Stromversorgung
- 8 Anlagen in Gasversorgung
- 10 Anlagen in Kraftstoff- und Heizölversorgung
- 4 Anlagen in Fernwärmeversorgung

→ diverse → **Betreiber kritischer Anlage (KRITIS)**

Einrichtungen und Betreiber Digitale Infrastruktur



Einrichtungen

- IXP-Betreiber
- Managed Security Services Provider
- DNS-Dienstanbieter
- CDN
- TLD Registry
- Cloud-Computing-Dienste
- Betreiber öfftl. TK-Netze
- Rechenzentrumsdienste
- Managed Services Provider
- Vertrauensdiensteanbieter
- Betreiber öff. elektr. Kommunikationsdienste

- Mind. 250 Mitarbeiter
- >50 Mio Umsatz + >43 Mio Bilanz

→ Besonders wichtige Einrichtung

- Mind. 50 Mitarbeiter
- >10 Mio Umsatz + Bilanz

→ Wichtige Einrichtung

→ TK-Anbieter oder Netz (TKG) - separat

ESA → DORA Kritische IKT-Betreiber

Betreiber

- Zugangsnetz 100.000 TNA
- TLD Registry 250.000 Domains
- IXP 100 angeschl. Systeme
- Übertragungsnetz 100.000 Vertragspartner
- Serverfarm 10.000 phys. Instanzen, 15.000 virt. Instanzen
- Seekabelanlandestationen 1 angebundenes Kabel
- DNS-Resolver 100.000 Vertragspartner
- Vertrauensdienste 500.000 ausgestellte qual. Zertifkate, 10.000 ausgestellte öfftl. Serverzertifikate
- Rechenzentrum 3,5 MW Leistung
- CDN 75 Tbyte/Jahr
- Autoritativer DNS-Server 250.000 Domains

→ Betreiber kritischer Anlage (KRITIS)

Pflichten für Unternehmen im NIS2UmsuCG

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.

- besonders wichtig
- wichtig
- kritische Anlagen
- Ausnahmen

Änderungen an EnWG und Sicherheitskatalogen

EnWG

- EnWG wird durch NIS2 angepasst
- Bisherige Regelungen in §11 (1a)-(1g) aufgehoben
- Neuer § 5c IT-Sicherheit im Anlagen- und Netzbetrieb enthält Regelungen mit NIS2-Anpassung

Kataloge

- Sicherheitskataloge werden angepasst: neue Kataloge §5c (1) und (2) EnWG-E vorgesehen
- Bisherige Pflicht zur ISMS-Implementierung und Zertifizierung bleibt vermutlich bestehen

§ 5c (1) (2) → Angemessener Schutz gegen Bedrohungen durch Umsetzung von IT-Sicherheitskatalogen, inkl. Beschaffungs- und Dienstleister-Steuerung

§ 5c (3) → IT-RM, ISMS, Incident Management, Business Continuity, Supply Chain, Zulieferer, Training, Kryptografie, MFA und SSO, Personalsicherheit, Access Management, Notfall-Kommunikation, SzA

entspricht den Maßnahmen aus §30 (2) BSIG-E plus §31 SzA

§ 5c (6) (7) → BSI zentrale Meldestelle, 24h/72h/30 Tage Fristen, inhaltliche Vorgaben, Zwischenmeldungen (notwendig: SOC/SIEM)

§ 5c (4) (5) → Dokumentation über Einhaltung von Sicherheitsanforderungen, Mängelbeseitigungspläne und -fristen

§ 5c (3) → Bestimmung von Format, Inhalt und Gestaltung der Dokumentation und zur Behebung von Sicherheitsmängeln, Regelungen zur regelmäßigen Überprüfung der Erfüllung

§ 5c (8) → Registrierung beim BSI, Benennung Kontaktstelle und ständige Erreichbarkeit

Änderungen an TKG und Sicherheitskatalog

TKG

- TKG wird durch NIS2 angepasst
- Bisherige §§ 165 - 168 enthalten Regelungen mit NIS2-Anpassung
- Neuer § 165 (2a) enthält §30-NIS2-Maßnahmen

Katalog

- Sicherheitskatalog wird durch NIS2-Änderungen nicht direkt berührt
- Anpassung des Katalogs möglich, noch unklar
- Bleibt (wohl) weiter relevant

§ 165 (2) → Maßnahmen nach Stand der Technik und (neu!) unter Berücksichtigung einschlägiger europäischer und internationaler Normen

- - - - - - - → *könnte die Tür zur verbindlichen Anwendung von ISO/IEC 27011 öffnen (analog Energiesektor)*

§ 165 (2a) → IT-RM, ISMS, Incident Management, Business Continuity, Supply Chain, Zulieferer, Training, Kryptografie, MFA und SSO, Personalsicherheit, Access Management, Notfall-Kommunikation

→ entspricht den Maßnahmen aus §30 (2) BSIG-E

§ 168 (1)–(3) → BNetzA und BSI beide Meldestelle, 24h/72h/30 Tage Fristen, inhaltliche Vorgaben, Zwischen-meldungen (notwendig: SOC/SIEM)

- - - - - - - - - - → *Keine Neuerungen im Hinblick auf Dokumentation und Nachweise*

Pflichten und Sektorpflichten

NIS2 und EnWG ab 2024

Stadtwerk

Governance | Leitung | Entwicklung

Stromversorgung (kDL aus BSIG)

Straßenbahn (non-NIS2)

Energieanlage (EnWG)

Prozesse | Prozesse | Prozesse | Prozesse

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

Standorte | Standorte | Standorte

Externe | Personal | Wartung | Betriebsmittel

Energieanlage (EnWG)
- §5c EnWG-E Vorgaben (Sicherheit)
- IT-Sicherheitskatalog-neu BNetzA

Kritische Anlage (NIS2 und DachG)
- Resilienz aus KRITIS-DachG
- Registrierung

Einrichtung Energie (NIS2)
- Registrierung
- RM-Pflichten durch SiKat Energie?

Straßenbahn (ÖPNV) nicht NIS2
- NIS2-Pflichten etwas unklar
- Möglicherweise trotzdem betroffen

DORA-Pflichten für kritische IKT-Dienstleister

Risikomanagement

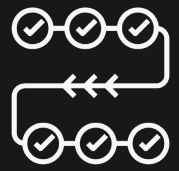
Detektion, Reaktion

Schutz der IT

Test und IKT-Audits

Physische Sicherheit

Governance

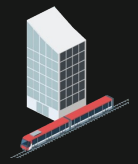


Interoperabilität

Standards

! Kritische IKT-Dienstleister können zusätzliche Pflichten über Verträge oder durch Einbezug in Resilienztests von Finanzunternehmen erhalten. Durch die Verpflichtung von Finanzunternehmen, Dienstleister zu steuern und Risiken von Drittparteien zu managen entstehen auch Auswirkungen auf nicht kritische IKT-Dienstleister.

NIS2 und DORA-Dienstleistungen



Registrierung

Meldung von Sicherheitsvorfällen

Einstufung als kritisch & Überwachung

IT-Provider

Governance | Leitung | Entwicklung

Dienstleistung (NIS2) | Dienstleistung (non-NIS2) | Dienstleistung (NIS2 und DORA)

Produkte | Produkte | Produkte

Prozesse | Prozesse | Prozesse | Prozesse

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

Colocation | Hyperscaler | Rechenzentren

Externe | Personal | Wartung | Betriebsmittel

NIS2-Einrichtung

Risiko-Management NIS2
+ Security Maßnahmen
+ Pflichten (Registrierung, Meldungen)

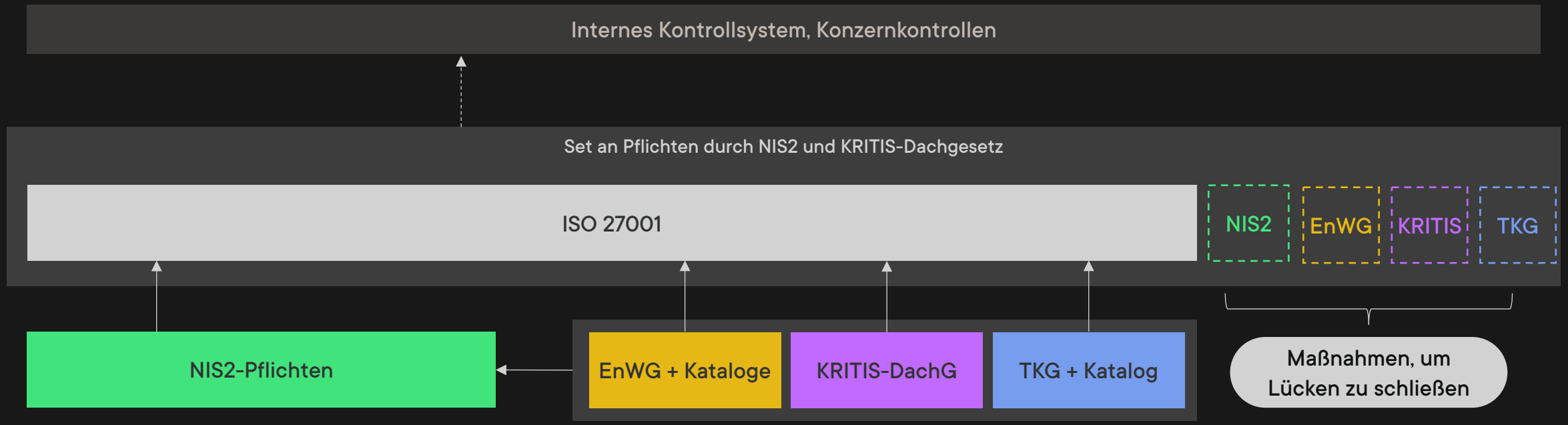
Einrichtung aber non-NIS2 Service

Wahrscheinlich auch NIS2-Scope

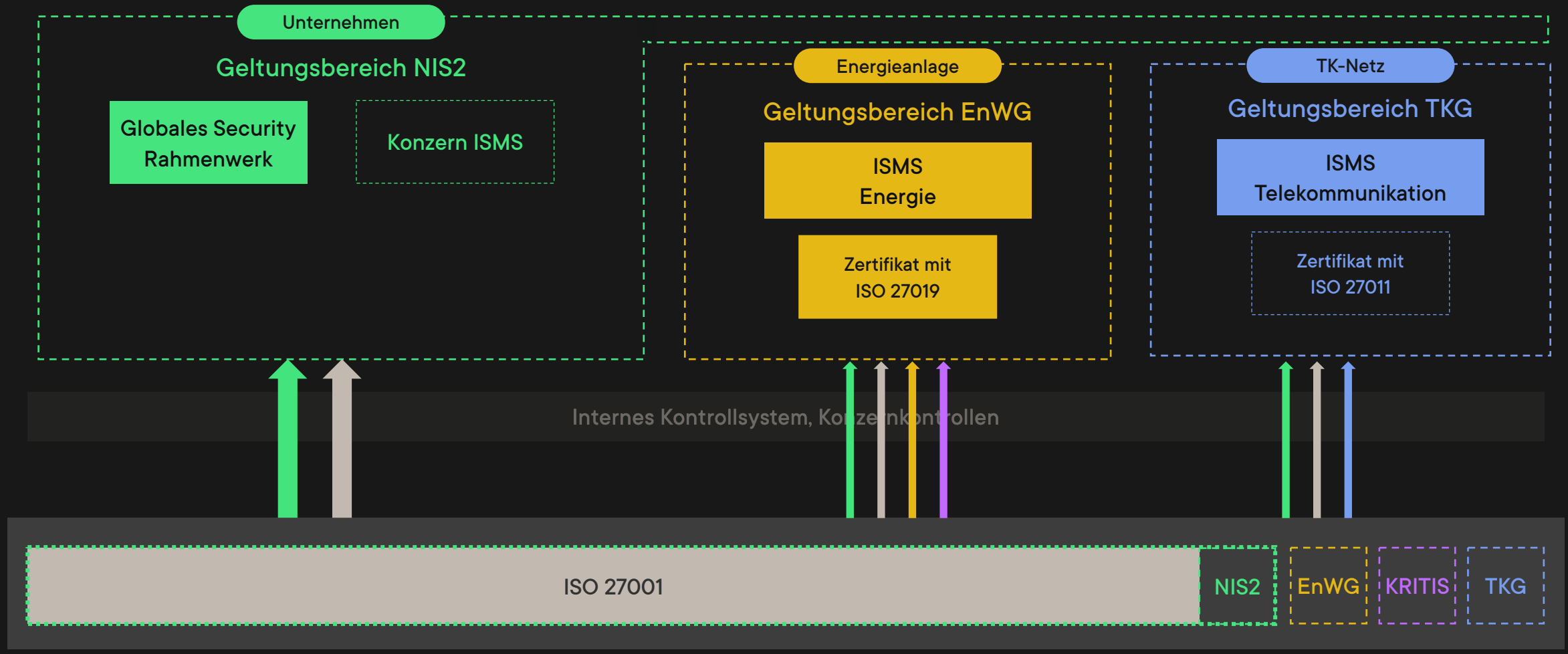
DORA IKT-Dienstleister (kritisch)

DORA-Pflichten Art. 33 (IKT)
+ Stresstests, Pentests
+ Vertragliche Pflichten durch Finanz

Kontrollmapping für Sektoren

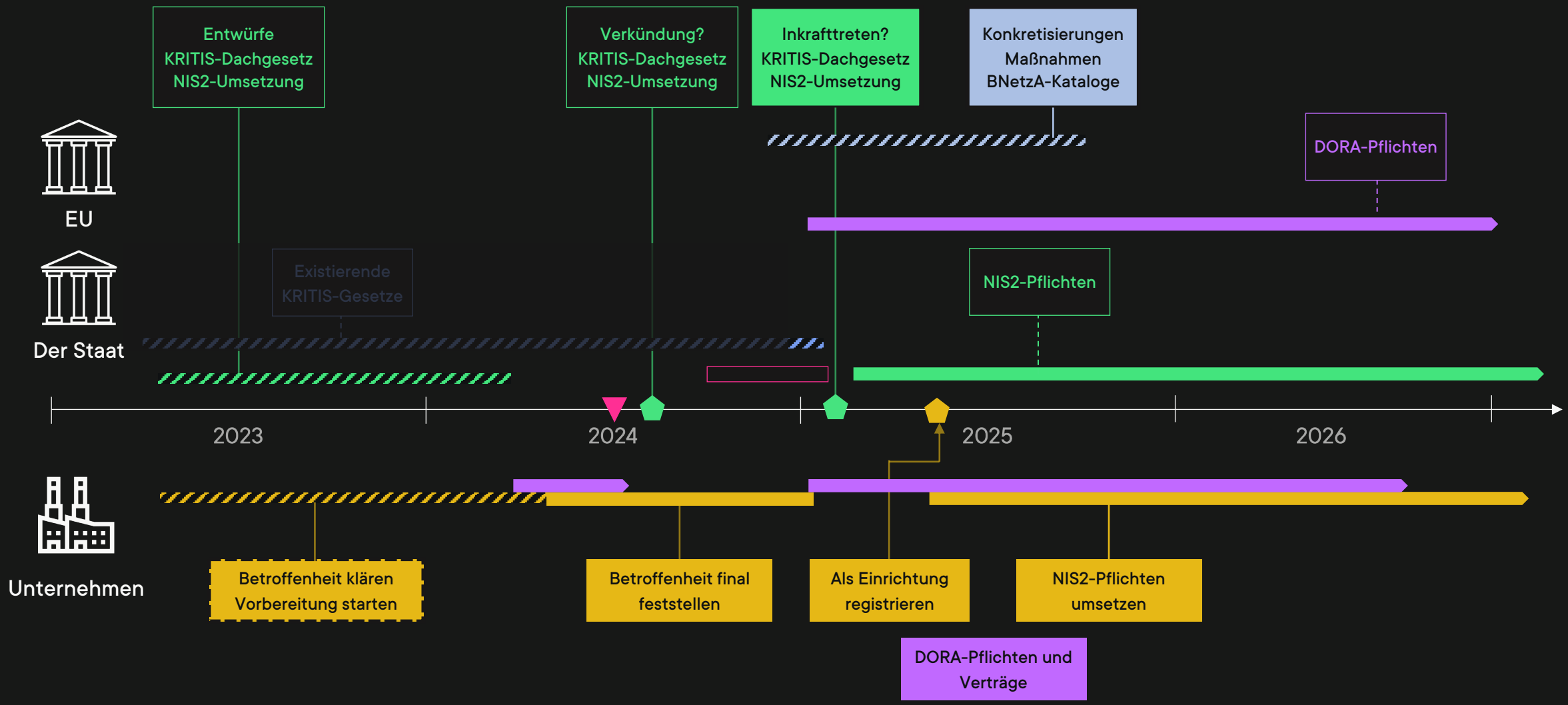


Mapping auf ISMSe



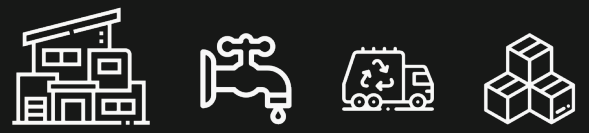

Und nun?

NIS2 und KRITIS ab 2024



Split Personalities – KRITIS und NIS2

Ein Stadtwerk



Verwaltung Wasserwerk Entsorgung Handel

Bei Überschreiten der Schwellenwerte in einer Anlage der KRITIS-Verordnung, z.B. Gewinnungsanlage >22 Mio. m^3/Jahr

Kritische Anlage

- ISMS im KRITIS-Scope aufbauen
- BCMS im KRITIS-Scope aufbauen
- NIS2, KRITIS-DachG, SzA-Maßnahmen
- Meldepflichten BSI und BBK
- Prüfungen und Nachweise

Personal
Dienstleister
Berater
!

Unternehmensgröße in einem der NIS2-Sektoren im NIS2-Umsetzungsgesetz, z.B. Wasserversorgungsanlage mit >50 MA

Einrichtung

- ISMS im Unternehmen aufbauen
- Vorbereitung auf Krisen, Ausfälle
- §30 NIS2-Maßnahmen
- Meldepflichten BSI
- Dokumentationspflicht

Es bleibt viel zu tun

Kontakt: info@openkritis.de und OpenKRITIS auf LinkedIn

Nichts zu Kritischen Infrastrukturen verpassen:

OpenKRITIS.de

Die OpenKRITIS-Konferenz 2024: openkritis.de/konferenz

KRITIS-Dachgesetz auf OpenKRITIS: KRITIS-Dachgesetz

NIS2-Umsetzung auf OpenKRITIS: NIS2 in Deutschland

Kontakt: info@openkritis.de und OpenKRITIS auf LinkedIn

NIS 2 und ISMS

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

EU NIS2 Mehrfach-Regulierung
Stand: 3. Juli 2024
Version: 1.0

Impressum

Insignals GmbH
Paul Weissmann
Rheinwerkallee 6
53227 Bonn

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

info@openkritis.de · +49 176 58952135