OpenKRITIS

NIS2 und KRITIS verspäten sich – Prüfungen

7. DIIR Digitale Tage 2025

NIS2 und KRITIS

Cybersecurity Prüfungen

Neue KRITIS-Regulierung EU 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

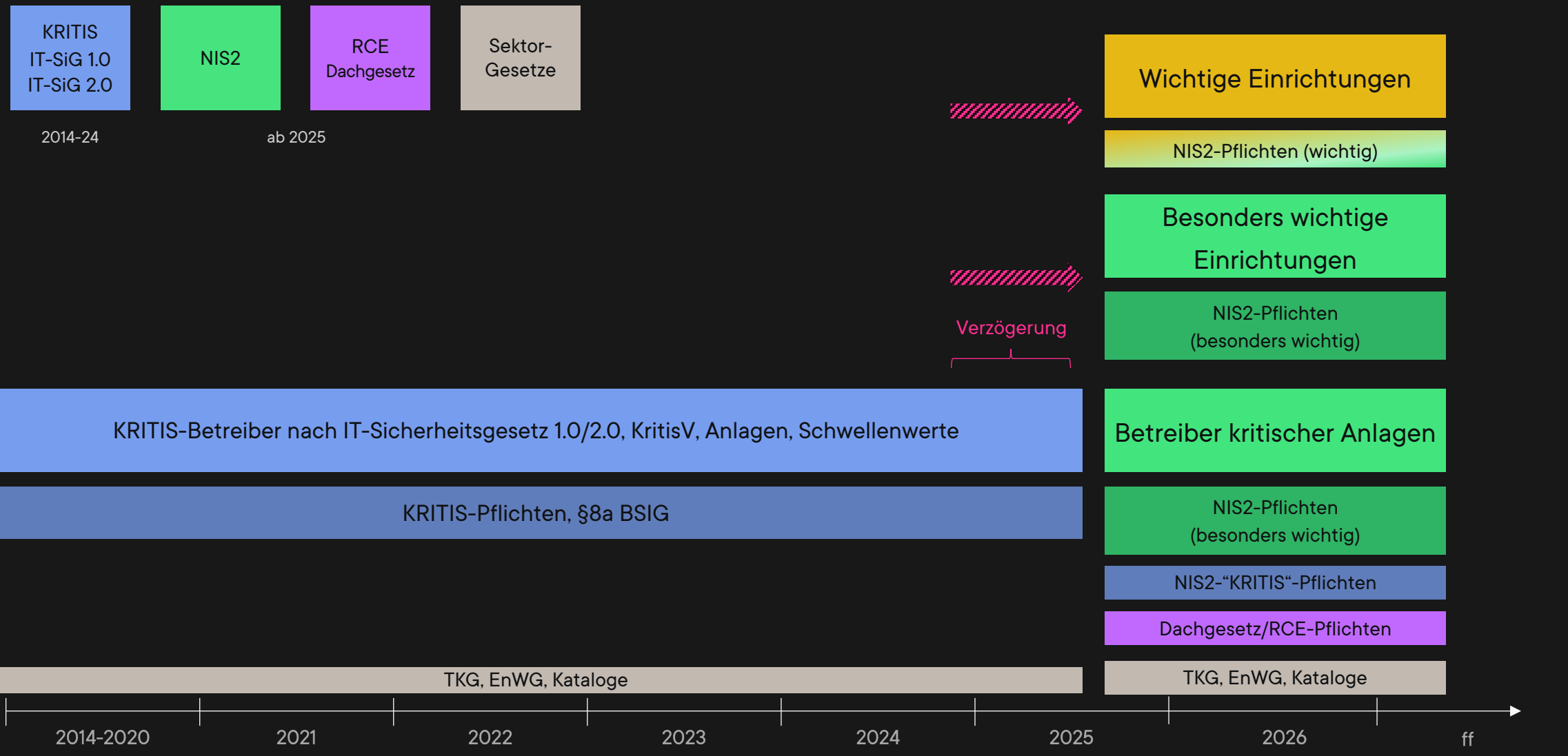
ab 2025
~~ab 10/2024~~

Bundesamt für Sicherheit in der Informationstechnik

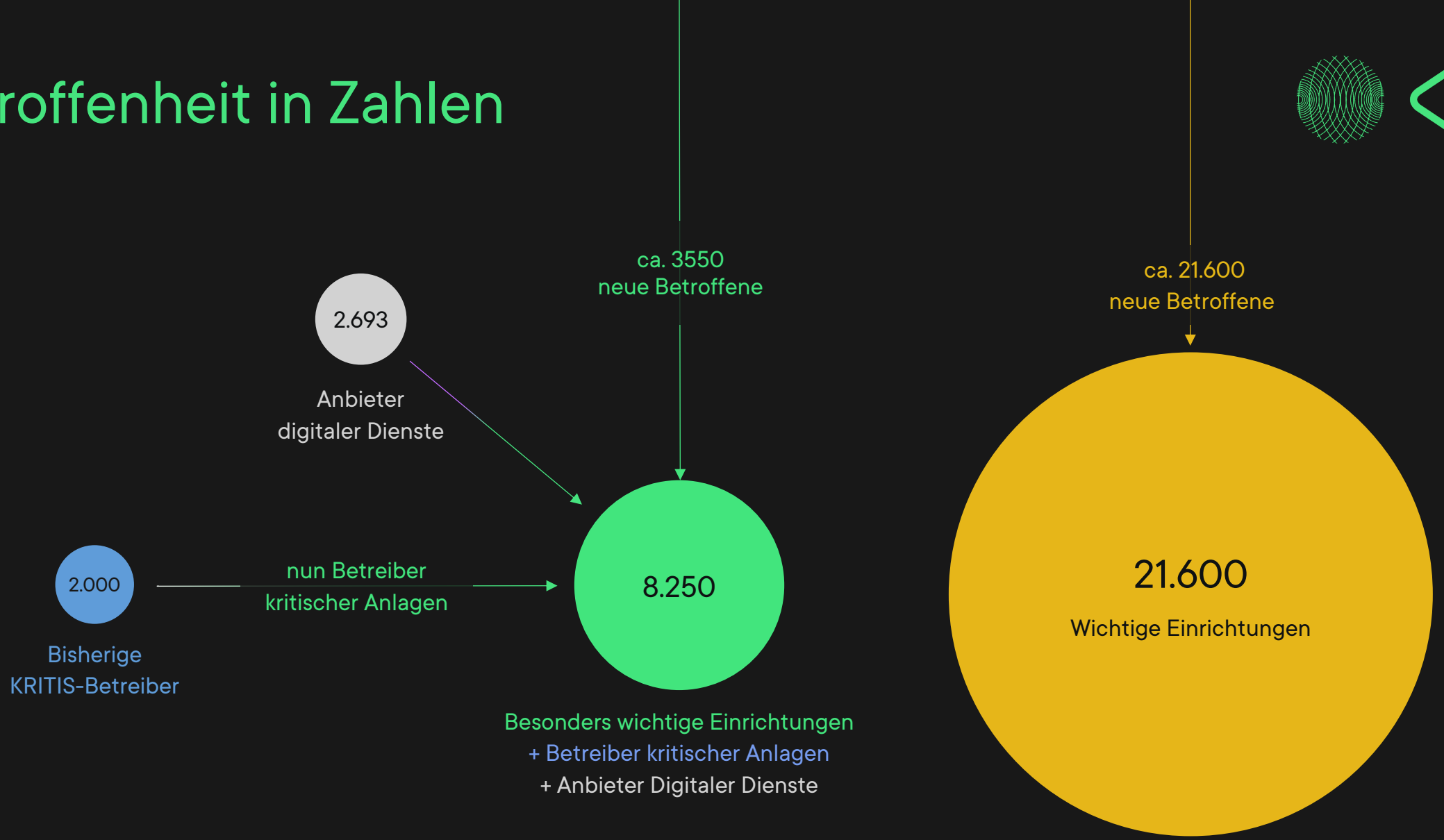
EU NIS2 → Umsetzung durch → NIS2UmsuCG

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

Kritische Infrastrukturen in Deutschland



Betroffenheit in Zahlen



Erfahrung anderer EU-Länder:
Deutlich mehr Unternehmen

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

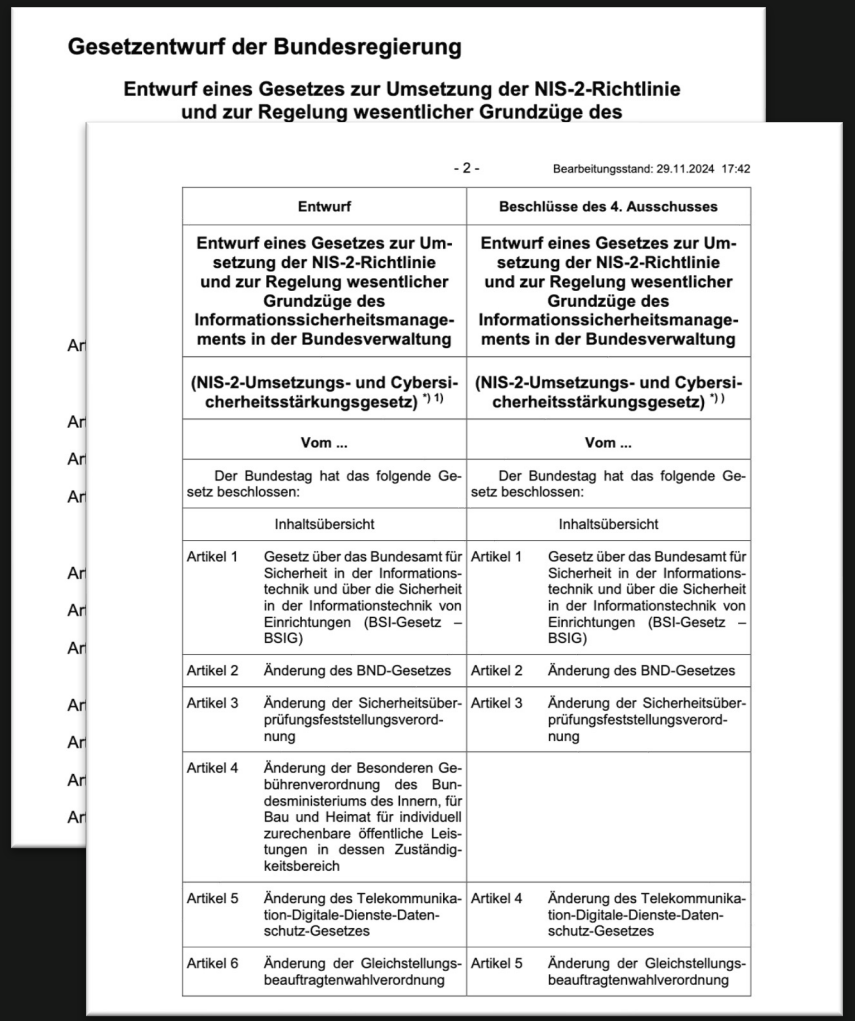
- Energie
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser
- Digitale Infrastruktur
- Siedlungsabfallentsorgung
- Weltraum
- Ernährung
- Bundeseinrichtungen

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

EU vs. DE

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

Status:

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

Notwendig für NIS2:

- Regierungsbildung
- Koalitionsvertrag und Agenda
- Ministeriumsverteilung

Vermutungen:

- Gesetz ähnlich wie letzte Entwürfe
- Viele DE-Anpassungen aus Q4 2024 = ?
- Grundsatz ist klar (EU RL), Timing 2025 H2?

NIS2 und KRITIS
Cybersecurity
Prüfungen

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)
- 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

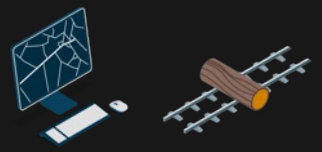
- Nachweise auf Nachfrage der Aufsichtsbehörde
- darf bei Zweifeln nachprüfen
- Audits (wie KRITIS)
- BBK macht Vorgaben zu Audit-Durchführung

§ 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

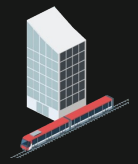
1 Monat

- 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

KRITIS-Geltungsbereich (bisher)



Allgemeinheit
>500. Tsd Bürger

Kunden

Kunden

IT-Konzern

Governance

Leitung

Entwicklung

Datenspeicherung
kritisch (kDL)

Telekommunikation
(unter Schwelle)

Autovermietung
(non-KRITIS)

Anlage CDN (BSIG)

Prozesse | Prozesse | Prozesse | Prozesse

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

Standorte | Standorte | Standorte

Externe | Personal | Wartung | Betriebsmittel

KRITIS-Anlage (BSIG 2021)

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

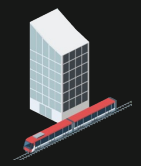
Weiterer Betrieb (non-KRITIS)

- ISMS und Maßnahmen nach Bedarf
- Schnittstellen

Vielleicht im KRITIS-Scope

- Verantwortung anteilig

Geltungsbereich mit NIS2



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,

NIS2 und KRITIS Cybersecurity Prüfungen

NIS2 und KRITIS-Prüfungen

KRITIS-Prüfungen
§8a BSIG

NIS2/KRITIS-Prüfungen
§39 BSIG-E

KRITIS-DachG
§16 KritisDG-E

bis 2025

ab 2026?

ab 2027?

KRITIS und Security

Prüfungen

- KRITIS-Betreiber
- Alle 2 Jahre
- Scope: KRITIS-Anlage
- Prüfgrundlage KdA/BSIG/SzA

KRITIS, NIS2 und Security

Prüfungen

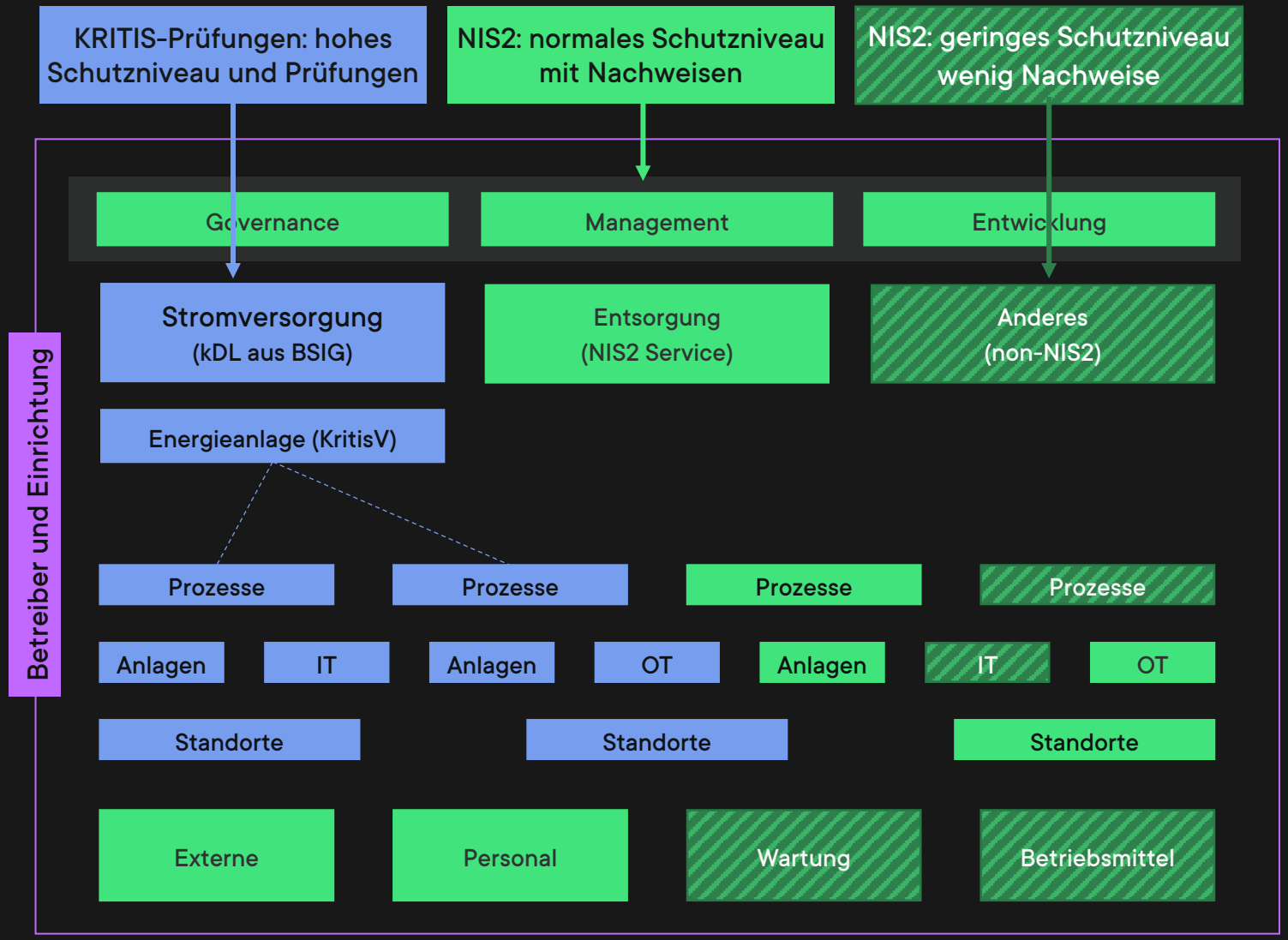
- NIS2 Kritische Anlagen
- Bestehende Zyklen + 1 Jahr
- Scope: Anlage (Einrichtung?)
- Prüfgrundlage in Arbeit/RUN
- Mit Dachgesetz-Nachweis

Resilienz

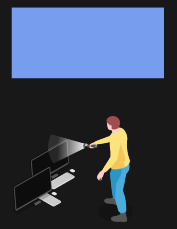
Nachweise

- KRITIS-Betreiber
- Übergangsfristen (2026+)
- Keine eigenen Prüfungen
- Scope: Anlage/Einrichtung?
- Prüfung: Teil von KRITIS/NIS2

NIS2 und KRITIS-Prüfungen: Scope



Prüfungen nach Schutzniveau



KRITIS-Prüfungen §8a bzw. §39 BSIG-E

- KRITIS-Anlage in NIS2 (kDL) - *tbc*
- Anforderungen KRITIS-NIS2
- Anforderungen KRITIS-Dachgesetz
- Umfangreiche Prüfmethodik
- Umfangreiche Prüfgrundlage

Nachweispflicht NIS2 mit Stichproben

- NIS2-Scope ganze Einrichtung
- Nachweise, Stichproben, int. Revision
- Controlset von (nur) NIS2

Anderes *nicht in NIS2*

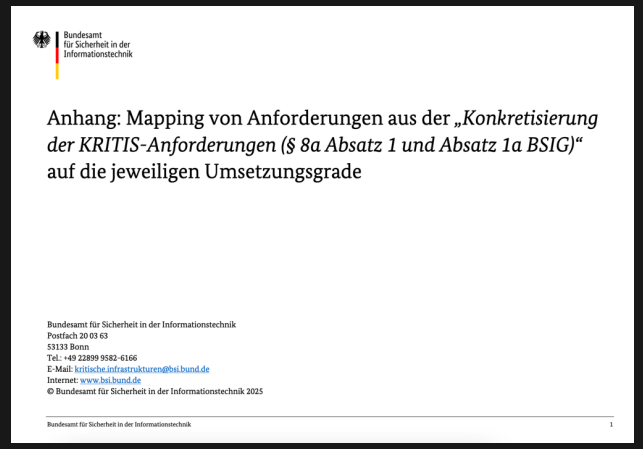
- NIS2-Scope für low-risk Assets
- Wenig Stichproben (selten)
- Wenig bis keine Nachweise

NIS2 und KRITIS-Prüfungen: Vorgaben

RUN Reifegrade

- Reifegrade in KRITIS
- ISMS/BCMS, plus neu:
- SzA/Tec/Org/Phy/Pers
- Erhebung durch Prüfer
- Kriterienkatalog BSI

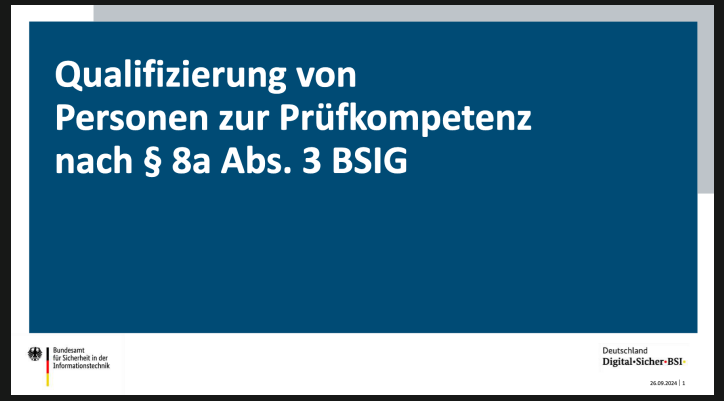
ab 4/2025



RUN und KdA

- Mapping Reifegrade KdA
- Neue Struktur KdA
- Integration SzA in KdA
- Einzelmapping auf Standards (in Arbeit)

ab 4/2025

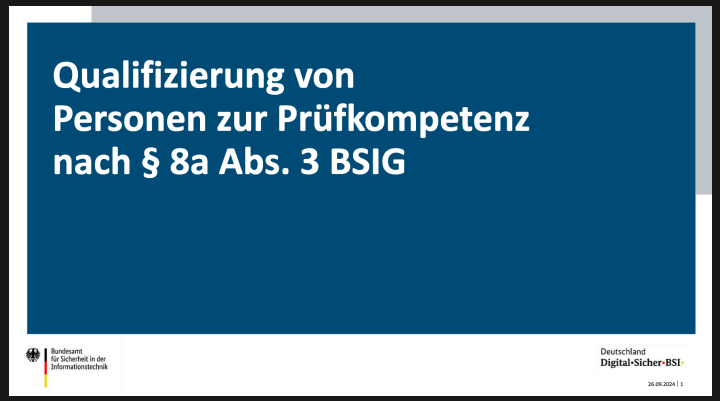


BSI-Prüfmethodik

- Qualifikation KRITIS-Prüfer
- Methodik für Prüfungen
- Von 2 auf 4,5 Tage + Zert.
- Prüfmethodik, Prüfteam
- Wirksamkeit, Stichproben

2025?

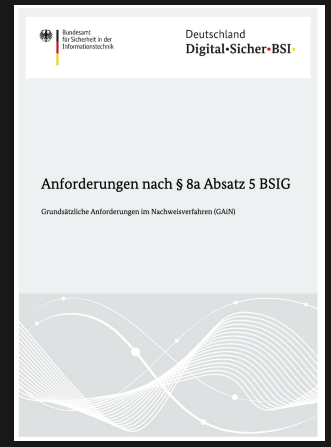
NIS2 und KRITIS-Prüfungen: Wirksamkeit und IR



BSI-Prüfmethodik

- Wirksamkeitsprüfung wird wichtiger!
- Methodik „analog PS 980“ (IDW)
- Stichproben (≈ PS 310), Prüftiefe
- Angemessenheit *und* Effektivität
- Verantwortung bei Prüfern

2025?



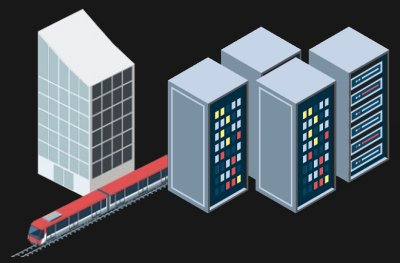
GAiN

- Anforderungen KRITIS-Prüfungen
- Mit: Vorgaben interne Revisionen
- Unabhängigkeit IR: IIA-Standards
- Quality Assessment IDW PS 983

bisher wenige interne KRITIS-Prüfer

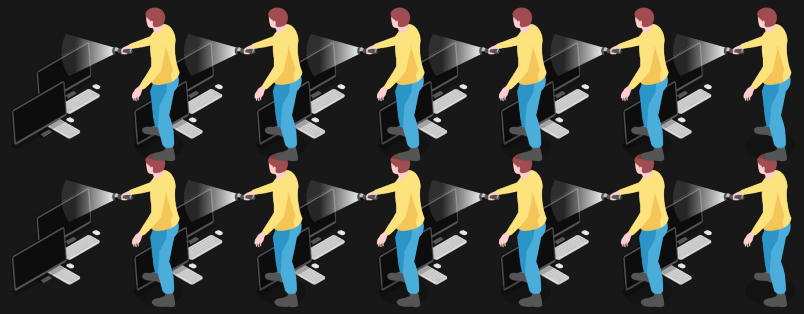
4/2025

NIS2 und KRITIS-Prüfungen: Prüfermarkt



Kritische Infrastrukturen

KRITIS-Prüfungen



Externe Prüfer

Unabhängig

Security-Expertise

Fachexpertise

Interne Revision

»Unabhängigkeit« ?

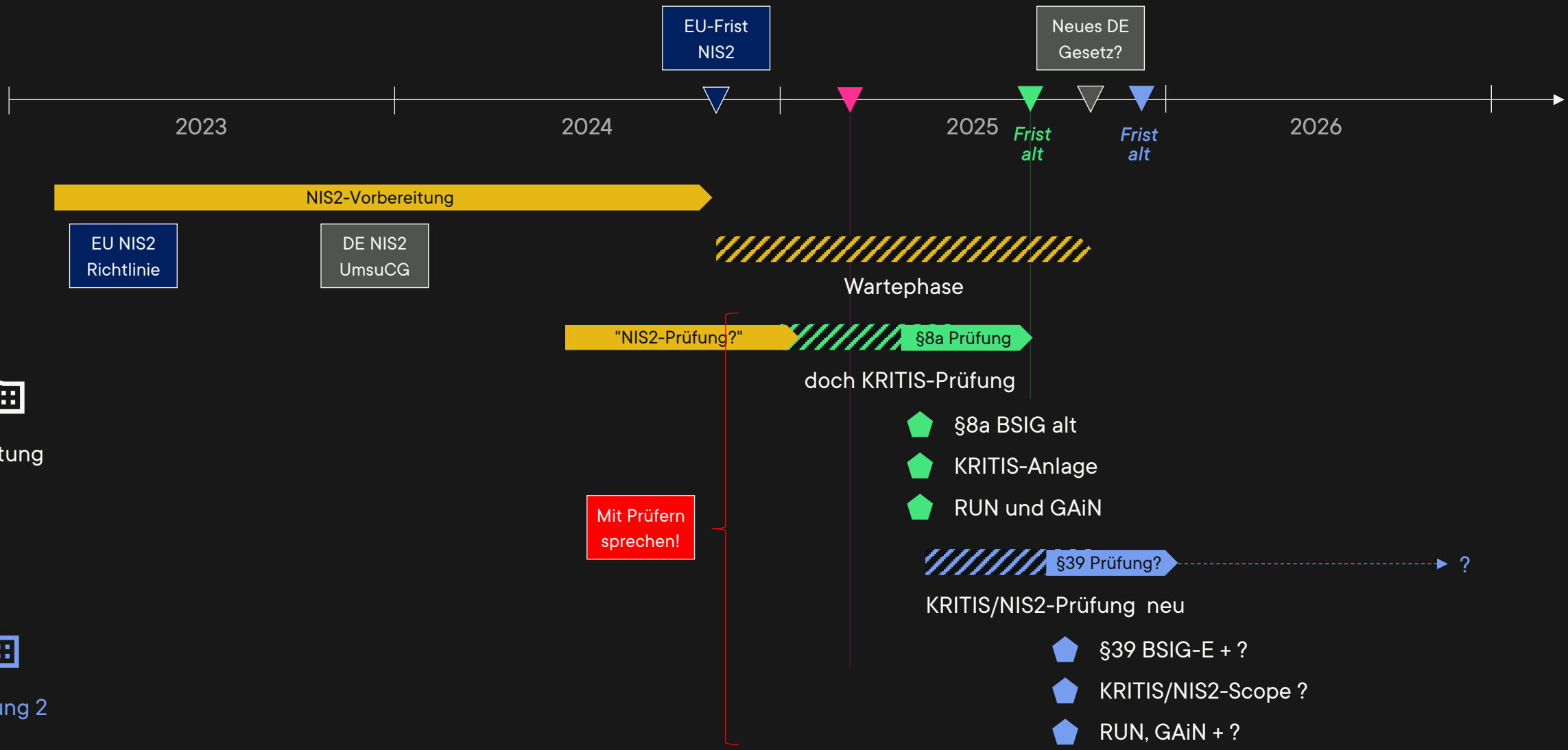
Betriebsexpertise

Vertrauen Unternehmen

NIS2 und KRITIS Cybersecurity Prüfungen

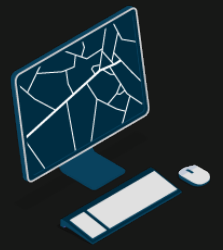
Und nun?

KRITIS und verzögerte Prüfungen



NIS2: Was tun 2025?

Compliance
Gesetze, ISMS, Governance



Cybersecurity
Technische Themen, IT/OT

Personal
Experten, Berater, Prüfer

Danke!

NIS2 und Prüfungen

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

EU NIS2 und KRITIS-Dachgesetz in Prüfungen
Stand: 17. März 2025
Version: 1.2

Impressum

Insignals GmbH
Paul Weissmann
Rheinwerkallee 6
53227 Bonn

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

info@openkritis.de · +49 176 58952135