Deloitte.

Aktuelles zu NIS-2 und KRITIS Dachgesetz

25. Juni 2025

Agenda

IT-Sicherheitsregulierung in a nutshell

Betroffenheitsanalyse

Pflichten

Summary: Vorbereitung zur Umsetzung

Fragen

IT-Sicherheitsregulierung in a nutshell

Aktuelle und zukünftige IT-Sicherheitsregulierungen auf EU- und Bundesebene [Auszug]

Die EU-Richtlinien sowie europäische Umsetzungsgesetze erweitern den bestehenden regulatorischen Rahmen im Bereich Cybersicherheit und Resilienz

NIS2 Directive (EU) 2022/2555

- Seit 16. Januar 2023 in Kraft
- Cyber Security
- Essentials/Important Entities nach size-cap
- Nationale Aufsicht + EU

Critical Entities Resilience (CER) Directive (EU) 2022/2557

- Seit 16. Januar 2023 in Kraft
- Resilienz und BCM
- Critical Entities
- Nationale Aufsicht + EU

Implementing Regulation (EU) 2024/2690

- seit 18. Oktober 2024 in Kraft
- Konkretisierung der Risikomanagementmaßnahmen + Definition „erheblicher Sicherheitsvorfall“
- Ausgewählte Einrichtungsarten in den Branchen Digitale Infrastruktur, ICT Service Management, Digitale Dienste
- Zuständige nationale Aufsicht

IT-Sicherheitsgesetz 2.0

- seit 28. Mai 2021 in Kraft
- IT-Sicherheit
- KRITIS-Betreibe gem. KritisV
- Deutsche Aufsicht (BSI)

NIS2 UmsuCG

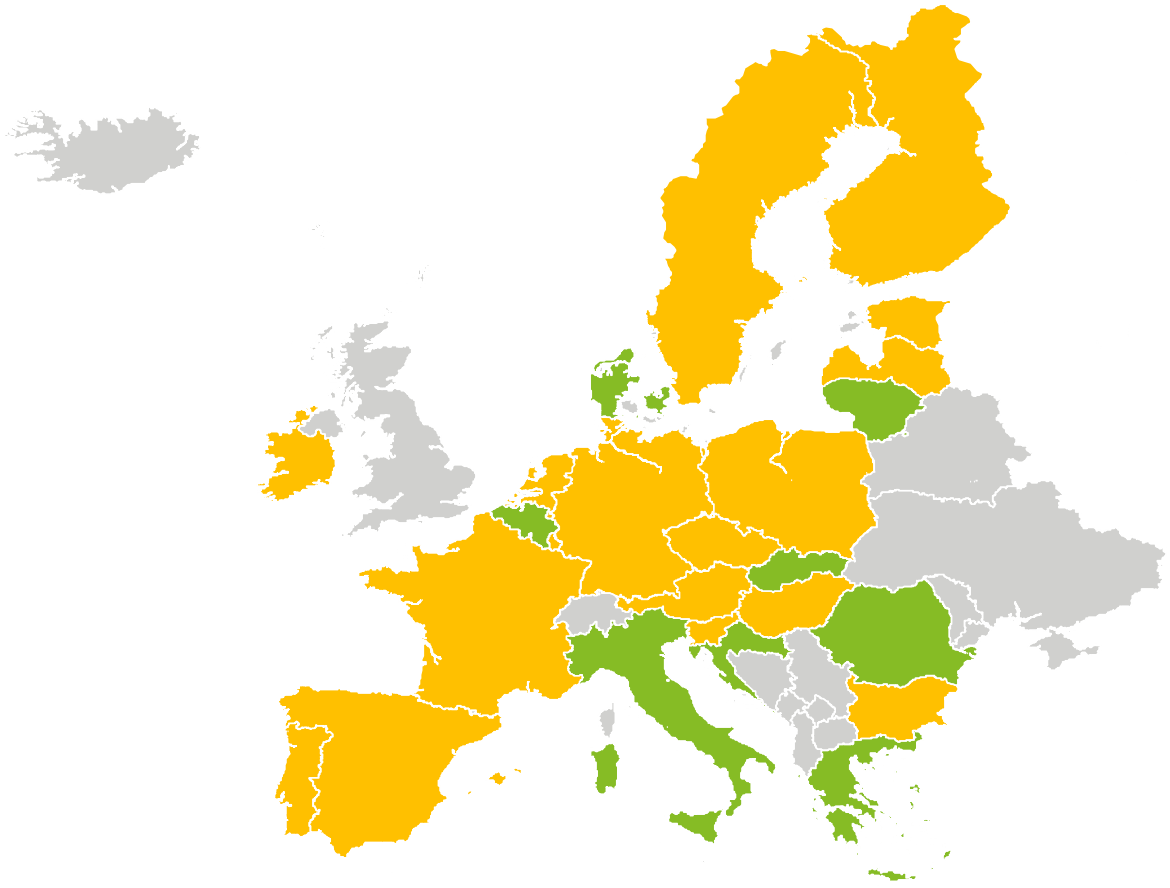
- Ende 2025
- Cyber-Sicherheit
- Wichtige und besonders wichtige Einrichtungen, KRITIS-Betreiber
- Deutsche Aufsicht (BMI, BSI)

KRITIS-Dachgesetz

- Januar 2026
- Physische Sicherheit
- KRITIS-Betreiber gem. KritisV
- Deutsche Aufsicht (BMI, BSI, BBK)

Umsetzungsstand NIS-2 auf EU-Ebene – Stand 07.05.2025

Eine Vielzahl der EU-Staaten hat die Richtlinie nicht fristgerecht zum 18. Oktober 2024 in die nationale Gesetzgebung überführt, inklusive Deutschland



NIS-2 bereits umgesetzt:

- Belgien, Kroatien, Dänemark, Griechenland, Italien, Litauen, Rumänien, Slowakei

NIS-2 noch nicht vollständig umgesetzt:

- Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Irland, Lettland, Luxemburg, Niederlande, Österreich, Polen, Portugal, Schweden, Slowenien, Spanien, Tschechische Republik, Ungarn, Zypern

Legende:

	Abgeschlossen
	In Arbeit/Entwurf
	Nicht in der EU

Gesetzgebungsverfahren: Vereinfachte Darstellung

Aufgrund des Diskontinuitätsprinzips[1] wurde das Gesetzgebungsverfahren für die Umsetzung der europäischen Regularien erneut begonnen

1. Referentenentwurf

Bundesministerium des Innern

- Erarbeitung eines ersten Gesetzesentwurfs innerhalb des zuständigen Ministeriums
- Beteiligung von Fachkreisen und Verbänden

2. Stellungnahmen: Länder/Verbändebeteiligung

Bundesländer, Verbände, Organisationen und Institutionen

- Einbindung anderer Ressorts
- Beteiligung der Bundesländer, Kommunen und Verbände

3. Kabinettsbeschluss (Regierungsentwurf)

Bundeskabinett = Bundesregierung

- Beschlussfassung über den abgestimmten Gesetzentwurf
- Offizielle Einbringung in den Bundestag

4. Bundestag

Bundestag

- 1. Lesung: Vorstellung des Gesetzentwurfs
- Ausschussberatungen (z.B. Innenausschuss, Wirtschaftsausschuss)
- 2. & 3. Lesung: Debatte & finale Abstimmung

5. Bundesrat

Bundesrat

- Prüfung des Gesetzes
- Ggf. Zustimmung oder Einspruch
- Falls erforderlich: Vermittlungsausschuss

6. Verkündigung & Inkrafttreten

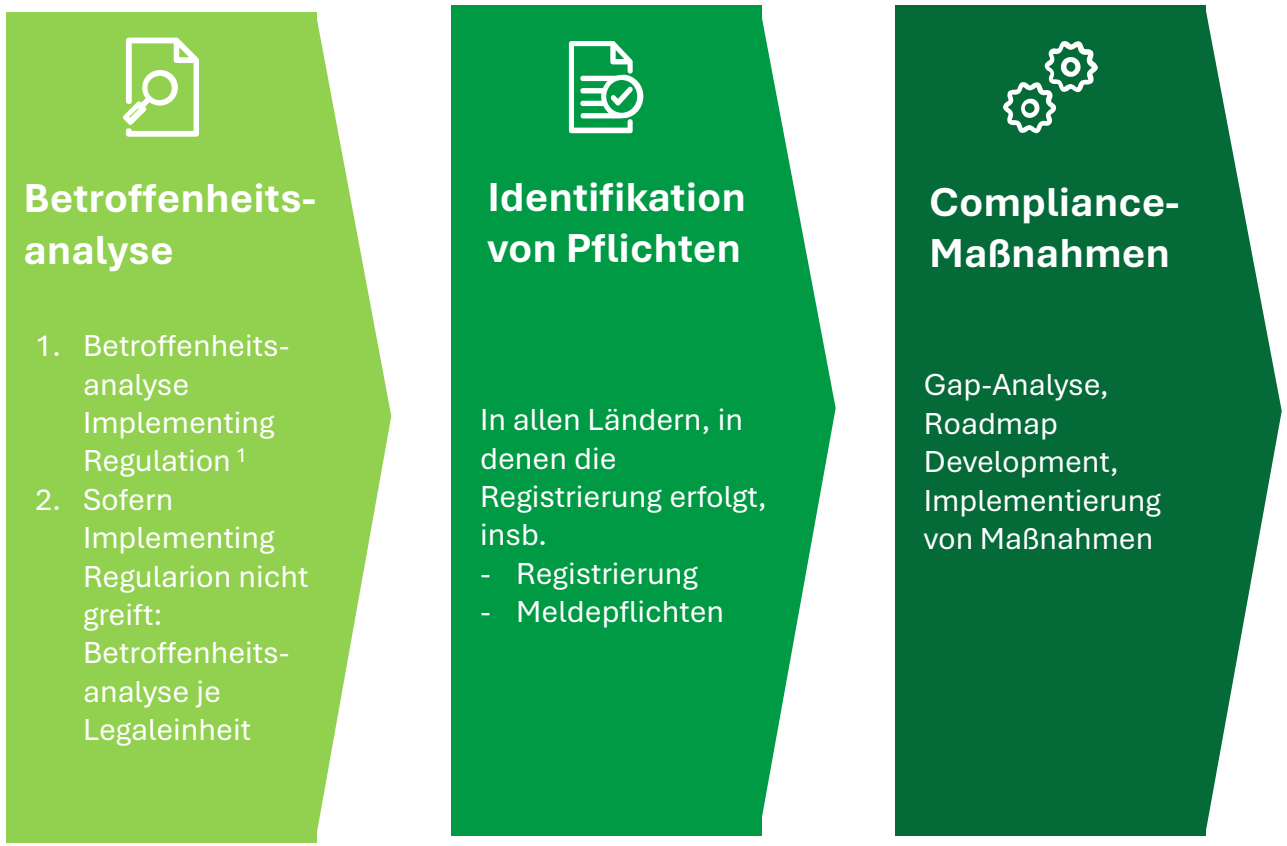
Bundesregierung / Bundespräsident

- Unterzeichnung durch den Bundespräsidenten
- Veröffentlichung im Bundesgesetzblatt
- Inkrafttreten gemäß gesetzlicher Regelung

[1] Die *sachliche Diskontinuität* besagt, dass Gesetzesvorhaben, die innerhalb einer Legislaturperiode nicht verabschiedet worden sind, nach Ablauf dieser Periode automatische Erledigung finden. Soll das Vorhaben weiterhin umgesetzt werden, muss das Gesetzgebungsverfahren – angefangen bei der Gesetzesinitiative – in der folgenden Legislaturperiode neu beginnen.
Dabei gilt die sachliche Diskontinuität auf Bundesebene nur für den Bundestag, nicht beispielsweise für den Bundesrat. Im Bundestag verabschiedete Gesetzesvorhaben können daher vom Bundesrat noch weiter behandelt und beschlossen werden.

Handlungsbedarf für Unternehmen

Die Durchführung einer Betroffenheitsanalyse und Ableitung der spezifischen Pflichten ist die Basis für die Compliance mit der kommenden IT-Sicherheitsregulierung



[1] DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider sowie für Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke

Betroffenheitsanalyse

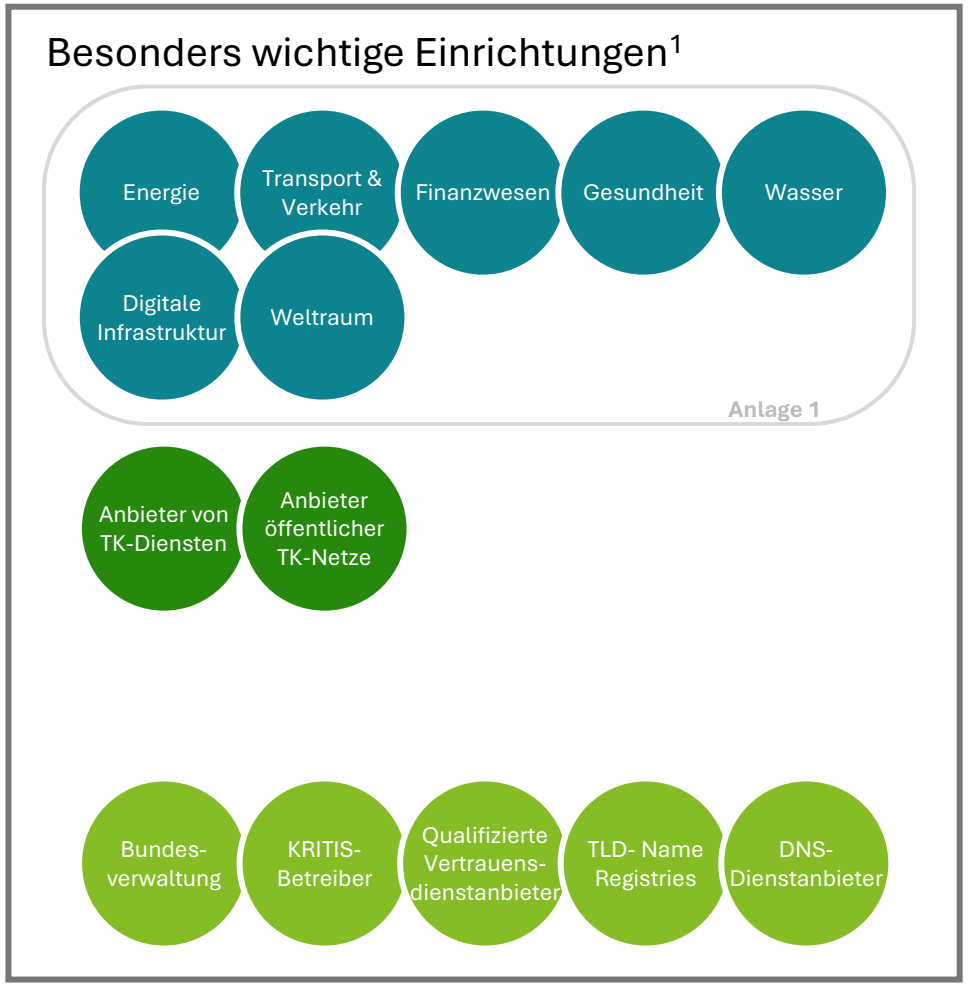
NIS-2-Betroffenheit

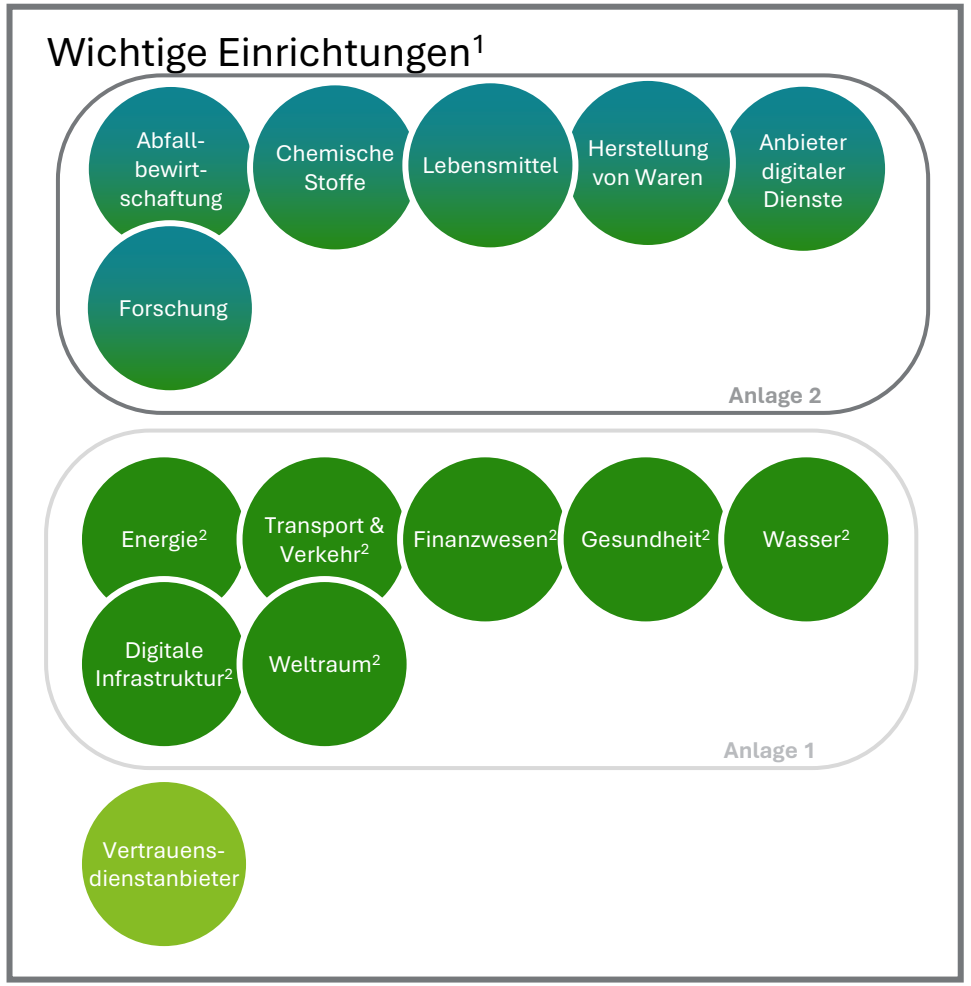
Die „besonders wichtigen" und "wichtigen" Einrichtungen erweitern den Anwendungsbereich bisheriger Regularien erheblich

Große Unternehmen
>250 Mitarbeiter oder
>50 Mio. EUR Umsatz
und
>43 Mio. EUR-Bilanz

Mittlere Unternehmen
>50 Mitarbeiter und
>10 Mio. EUR Umsatz
oder
>10 Mio. EUR-Bilanz

Größenunabhängig





Size cap Kriterium

Sektor/Branche/Einrichtungsart[1]

[1]Die betroffenen Branchen und Einrichtungsarten der entsprechenden Sektoren sind in Anlage 1 und Anlage 2 des NIS2-Umsetzungsgesetzes näher definiert. Es bestehen einige Ausnahmen, vgl. u.a. § 28 NIS2UmsuCG
[2]Sofern nicht bereits eine besonders wichtige Einrichtung.
Für Einrichtungen, die der Anlage 1 zuzordnen sind, entscheidet die Unternehmensgröße darüber, ob die Einrichtung wichtig oder besonders wichtig ist. Unternehmen

Betroffenheitsanalyse NIS-2: Auszug aus dem NIS2 UmsuCG, Referentenentwurf vom 23.06.2025

1. Sichtung des Paragraph § 28, Beispiel eines Unternehmens in der Stromversorgung

Auszug NIS2 UmsuCG

§ 28

Besonders wichtige Einrichtungen und wichtige Einrichtungen

(1) Als besonders wichtige Einrichtung gelten

1. Betreiber kritischer Anlagen,
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) mindestens 50 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,
4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die
   a) mindestens 250 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

Betroffenheitsanalyse: Auszug aus dem NIS2 UmsuCG, Referentenentwurf vom 23.06.2025

2. Sichtung der referenzierten Anlagen und Querverweise in der Spalte der Einrichtungsart

Auszug NIS2 UmsuCG – Anlage 1

Anlage 1

Sektoren besonders wichtiger und wichtiger Einrichtungen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Energie**		
1.1		Stromversorgung	
1.1.1			Stromlieferanten nach § 3 Nummer 31c EnWG
1.1.2			Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 3 EnWG
1.1.3			Betreiber von Übertragungsnetzen nach § 3 Nummer 10 EnWG
1.1.4			Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG

Auszug EnWG

31c. Stromlieferanten
natürliche und juristische Personen, deren Geschäftstätigkeit ganz oder teilweise auf den Vertrieb von Elektrizität zum Zwecke der Belieferung von Letztverbrauchern ausgerichtet ist,

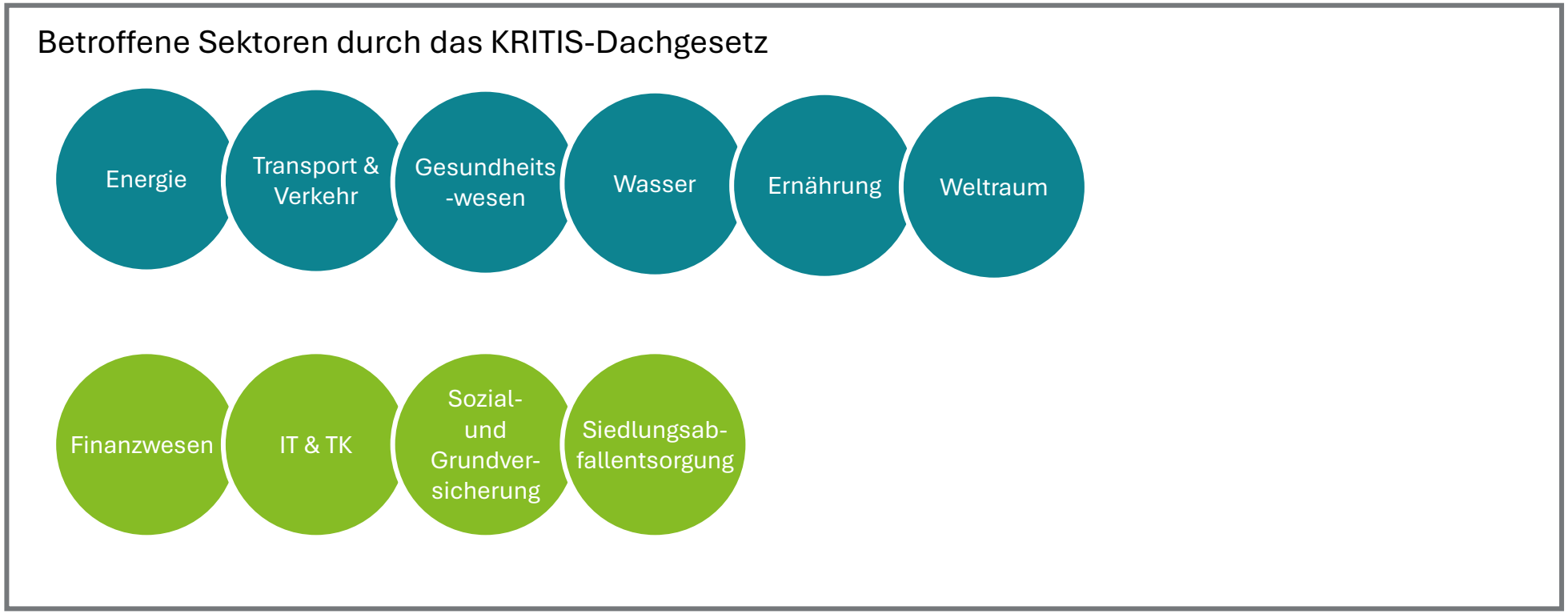
KRITIS-Dachgesetz-Betroffenheit

Mit dem KRITIS-Dachgesetz und NIS-2 werden neue Sektoren im Vergleich zur bisherigen KritisV eingeführt

> 500.000 von einer Anlage zu versorgende Einwohner (< 500.000 bei funktionaler Bedeutung (z. B. Alleinstellung, Abhängigkeiten, Region) nach §5 Abs. 3)

Unabhängig von Einwohnerzahl

Schwellenwerte



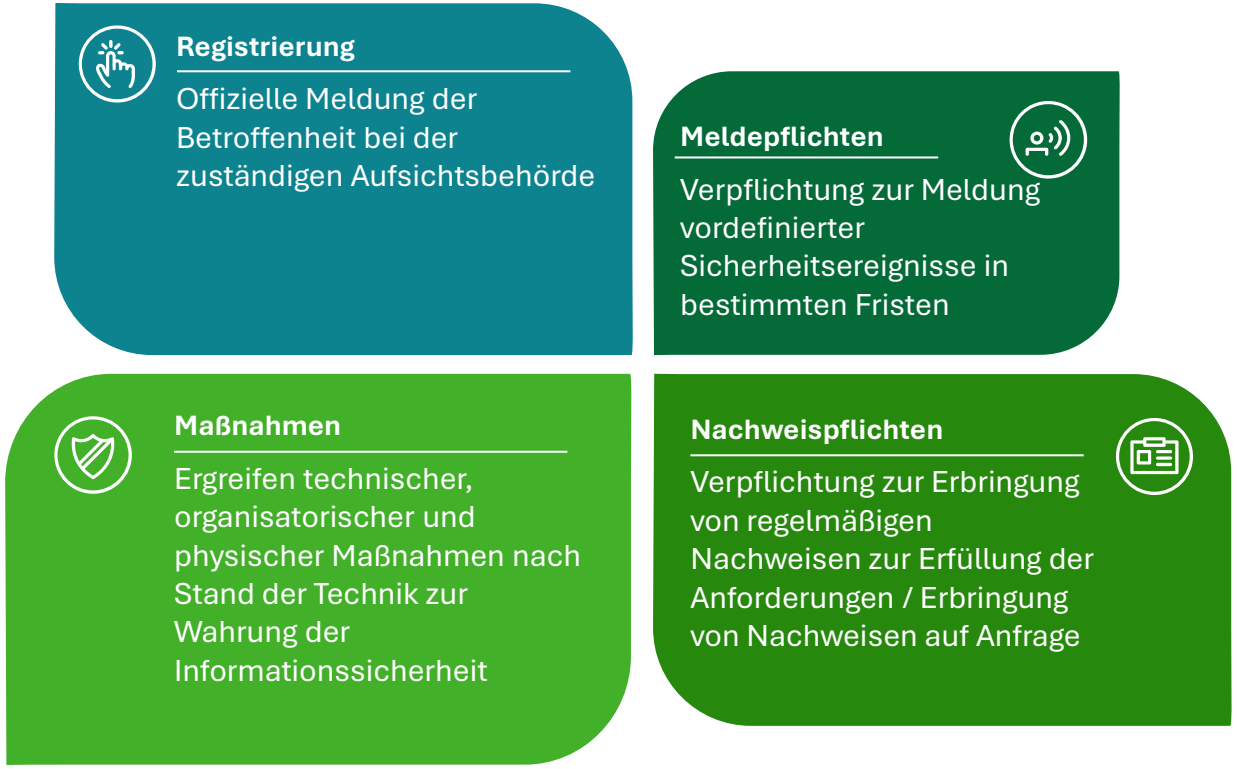
Sektor/kritische Dienstleistung/Anlage[1]

[1]Gemäß §4 (3) bestimmt das Bundesministerium des Innern und für Heimat bestimmt durch eine Rechtsverordnung, die kritischen Dienstleistungen, die jeweils zu den Sektoren nach Absatz 1 gehören

Pflichten

Pflichten IT-Sicherheitsregulierung

Die mit IT-Regulierung einhergehenden Pflichten umfassen Registrierungspflichten, Meldepflichten, Pflichten zum Ergreifen von Maßnahmen sowie Nachweispflichten



NIS-2 Registrierungs- und Meldepflichten

Neben der Registrierung betroffener Unternehmen wird ein dreistufiges Meldeverfahren für die Erfassung von Sicherheitsvorfällen durch das BSI eingeführt

Registrierungspflichten

Besonders wichtige Einrichtungen sowie wichtige Einrichtungen und Domain-Name-Registry-Dienstanbieter sind nach § 33 verpflichtet, sich spätestens **drei Monate nach Erstnennung oder erneuter Nennung bei einer noch einzurichtenden Registrierungsstelle des BBK und BSI zu registrieren**.

Angaben

1. Name der Einrichtung, Rechtsform, Handelsregisternummer
2. Anschrift, Kontakt (E-Mail, IP-Adressbereiche, Telefon)
3. Relevanter in Anlage 1 und 2 genannte Sektor
4. Auflistung der EU-Mitgliedsstaaten in denen die Einrichtung Dienste erbringt
5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.

KRITIS-Betreiber haben darüber hinaus die IP-Adressbereiche der von ihnen betriebenen Anlagen, sowie Anlagekategorie und Versorgungskennzahlen zu benennen

Meldepflichten

Das NIS2UmsuCG definiert mehrere Arten von Vorfällen (§ 2):

1. **Erheblicher Sicherheitsvorfall** (Schwerwiegende Störung/Verluste)
2. **Sicherheitsvorfall** (Beeinträchtigung der Schutzziele)
3. **Beinahevorfall** (verhinderter oder nicht-eingetretener Vorfall)
4. **Erhebliche Cyberbedrohung** (Potenzial für erheblichen Schaden)

Meldung

Meldung erheblicher Sicherheitsvorfälle an das BSI in Stufen (§ 32):

- Erstmeldung innerhalb von 24h nach Kenntniserlangung
- Bestätigungsmeldung zur Aktualisierung innerhalb von 72h
- Zwischenmeldung auf Anweisung des BSI
- Abschlussmeldung spätestens nach einem Monat

Unterrichtung

- **Bei erheblichen Sicherheitsvorfällen (§ 35):** BSI kann Einrichtungen anweisen, Kunden zu unterrichten
- **Bei erheblichen Cyberbedrohungen:** Mehrere Sektoren müssen Kunden und BSI über potenzielle Bedrohungen unverzüglich informieren

NIS-2 Maßnahmen

Die erforderlichen Maßnahmen nach §30 betreffen nahezu alle Mitarbeiter und Fachbereiche in einem Unternehmen, sodass ein strategisches und ganzheitliches Vorgehen unumgänglich ist

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, **geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen**, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den **Stand der Technik einhalten**, die einschlägigen **europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen**.

NIS-2 Maßnahmen

Das NIS2UmsuCG gibt folgende Mindestmaßnahmen vor

Mindestmaßnahmen nach § 30

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik

2. Bewältigung von Sicherheitsvorfällen

3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wieder-herstellung nach einem Notfall, und Krisenmanagement

4. Sicherheit der Lieferkette Einschl. sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung, Wartung von informations-technischen Systemen, Komponenten Prozessen, einschließlich Management und Offenlegung von Schwachstellen

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-maßnahmen im Bereich der Sicherheit in der Informationstechnik

7. Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik

8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,

9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und Für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Text-kommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

NIS-2 Nachweispflichten

Die Umsetzung der Maßnahmen muss von den Betreibern kritischer Anlagen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachgewiesen werden

Nachweispflicht:

Nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1:

Nachweis der Umsetzung der Maßnahmen:

1. Betreiber übermitteln die Ergebnisse der Audits, Prüfungen oder Zertifizierungen inkl. Aufgedeckter Sicherheitsmängel an das Bundesamt;
2. **Anforderungen einhalten:**
   - Art und Weise der Durchführung
   - Eignung der erbrachten Nachweise

Dokumentation

Das Bundesamt kann die Vorlage von Dokumentationen verlangen:

- Dokumentation der Prüfung (Prüfungsgrundlage)
- Vorlage eines geeigneten Mängelbeseitigungsplanes, wenn Sicherheitsmängel identifiziert wurden
- Nachweis über erfolgte Mängelbeseitigung

Häufigkeit

- Frühestens drei Jahre nach erstmaliger Benennung als Betreiber einer kritischen Anlage
- Spätestens drei Jahre nach erneuter Nennung als Betreiber einer kritischen Anlage
- Anschließend alle drei Jahre

NIS-2 Mehrfachregulierung und Differenzierung zwischen den unterschiedlichen Einrichtungen

Je nach Einrichtungsart greifen unterschieldiche Pflichten

Pflicht	Betreiber kritischer Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
Geltungsbereich	Anlage(n)	Unternehmen	Unternehmen
Maßnahme Risikomanagement §30	•	✓	✓
Höhere Maßstäbe für KRITIS §31 (1)	✓		
Besondere Maßnahmen SzA §31 (2)	✓		
Meldepflichten §32	•	✓	✓
Registrierung §33 §34	✓	✓	✓
Unterrichtungspflichten (Kunden) §35	•	✓	✓
Leitungsorgane §38	•	✓	✓
Nachweise §39	✓	tw. (§64)	tw. (§65)

Pflichten KRITIS-Dachgesetz

Analog zum NIS2 UmsuCG diktiert das KRITIS-Dachgesetz zusätzliche Pflichten für Betreiber kritischer Anlagen

Registrierung

- Betreiber kritischer Anlagen müssen sich beim BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) registrieren.
- Spätestens 3 Monate nach Feststellung als kritisch, jedoch frühestens bis 17.07.2026 (§ 8 KRITIS-DachG).
- Angaben: Name, Kontaktdaten, Sektor, kritische Dienstleistung, Versorgungsgrad, Kontaktstelle.
- Bei Unterlassung: BBK kann die Registrierung zwangsweise selbst vornehmen.

Meldepflichten

Gilt bei physischen Vorfällen, die kritische Dienstleistungen erheblich beeinträchtigen könnten (§ 18 KRITIS-DachG).

Beispiele:

- Naturkatastrophen, Sabotage, Stromausfall, Gebäudeschäden

Fristen:

- Unverzüglich, spätestens 24 Stunden nach Kenntnis: Erstmeldung.
- Nach 1 Monat: ausführlicher Abschlussbericht („Lessons Learned“).
- Meldung über die gemeinsame Plattform von BBK und BSI.

Maßnahmen

- Betreiber müssen einen Resilienzplan erstellen und regelmäßig aktualisieren (§ 13 KRITIS-DachG).

Inhalte sind u.a.:

- Zugangskontrollen, bauliche Sicherung, Detektionstechnik.
- Krisen- und Notfallmanagement.
- Alternativen zur Wiederaufnahme des Betriebs.
- Personal- und Objektschutzmaßnahmen.

Die Maßnahmen müssen verhältnismäßig und an die Risikoanalyse angepasst sein.

Nachweispflichten

Betreiber müssen auf Verlangen Nachweise erbringen (§ 16 KRITIS-DachG), z. B.:

- Resilienzplan
- Auditberichte
- Dokumentation von Maßnahmen.
- Grundlage ist ein risikobasierter Prüfansatz der Behörden.

Bei Mängeln:

- Anordnung von Nachbesserungspflichten, ggf. Bußgelder.

Gleichwertige Nachweise aus anderen Gesetzen (z. B. ISO-Zertifizierungen) können anerkannt werden (§ 17).

Non-Compliance bei NIS-2 und KRITIS

Darstellung verschiedener Verstöße und korrespondierender Bußgelder

Konsequenzen bei NIS-2 Non-Compliance

Bußgelder für Organisationen

KRITIS-Betreiber bis 2 Millionen Euro (bis NIS2);
besonders wichtige Einrichtungen: bis 10 Millionen Euro / 2% des weltweiten Umsatzes;
wichtige Einrichtungen: bis 7 Millionen Euro / 1,4% des weltweiten Umsatzes

Persönliche Haftung von Geschäftsführern

(wegen Verletzung von Genehmigungs- und Überwachungspflichten)

Konsequenzen bei Nicht-Einhaltung des KRITIS-Dachgesetzes

Bußgelder für Organisationen

Geringere Verstöße bis 100.000 Euro
Melde- und Registrierungspflichten verletzt bis 500.000 Euro

Bußgelder für Organisationen

Unvollständige/fehlerhafte Nachweise/Vorkehrungen bis 1 Millionen Euro
Nichtbefolgung gewisser behördlicher Anordnungen bis 2 Millionen Euro

Vorbereitung zur Umsetzung

Maßnahmen zur Sicherstellung der Compliance (Beispiel NIS-2)

Unsere bewährte Vorgehensweise basiert auf einem vierstufigen Ansatz, der die Vorgaben und Empfehlungen nationaler und internationaler Standards berücksichtigt

1
Betroffenheitsanalyse

- Analyse der Betroffenheit der Implementing Regulation
- Sofern die Implementing Regulation greift: Bestimmung der registrierungspflichtigen Hauptniederlassung
- Sofern die Implementing Regulation nicht greift: Analyse per Legaleinheit von NIS-2 (nationale Gesetzgebung!) betroffen ist, Auswertung der nationalen Gesetzgebung

2
Identifikation von Pflichten

- Sichtung der relevanten nationalen Gesetzgebung und der konkreten Pflichten je Einrichtungsart
- U.U. Miteinbezug der Implementing Regulation

3
Gap-Analyse

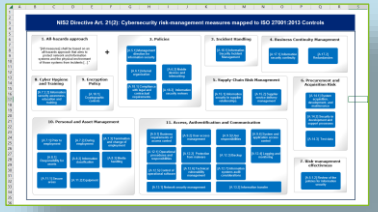
- Basierend auf einem geeigneten Compliance-Framework: Bewertung des Reifegrads der bestehenden Sicherheitsmaßnahmen in der Organisation und Ableitung notwendiger Handlungsfelder, die zur Herstellung der NIS-2 Compliance erforderlich sind

4
Roadmap Development

- Erarbeitung von Hanldungsempfehlungen, Implementierungsaktivitäten, -prioritäten und Zeitplänen im Einklang im IT-Strategie und –Zielbild
- Identifikation von Quick Wins und Hochrisikofeldern

5
Implementierung

- Einführung von Maßnahmen gemäß Roadmap, z.B. Definition von Rollen und Verantwortlichkeiten, Prozessdefinition, Erstellung von Richt- und Leitlinien



Ihre Ansprechpartner

Oliver Migge

Director | Hamburg
+49 151 580 021 60
omigge@deloitte.de

Janika Schauer

Manager | Hamburg
+49 151 580 703 71
janschauer@deloitte.de

Deloitte.