



KRITIS-Dachgesetz: Die wichtigsten Anforderungen

Vom Regelwerk zur Praxis – inkl. Compliance-Checkliste

Die aktuellen Anforderungen der CER-Richtlinie (EU 2022/2557) zur Stärkung der Resilienz von kritischen Anlagen

Die „Critical Entities Resilience“ – Directive (EU 2022/2557) wurde 2022 in der EU verabschiedet und ist in Deutschland am 17. März 2026 in Kraft getreten. Hierbei stellt das KRITIS-Dachgesetz (KRITIS-DachG) diverse Anforderungen an die physische Sicherheit sowie die Resilienz und Ausfallsicherheit von Unternehmen. So soll der physische Schutz die bestehenden IT-Sicherheitsmaßnahmen ergänzen.

Das Gesetz schafft erstmals bundesweit einheitliche Mindeststandards für den physischen Schutz kritischer Anlagen und verpflichtet die Betreiber u. a. zur Durchführung von Risikoanalysen sowie zur Erstellung von Resilienzplänen. Diese Maßnahmen müssen regelmäßig aktualisiert (im Bedarfsfall oder mindestens alle 4 Jahre) und gegenüber zuständigen Behörden nachgewiesen werden. Zudem bestehen Meldepflichten bei Sicherheitsvorfällen sowie die Pflicht zur Implementierung organisatorischer Maßnahmen und Verfahren zur Aufrechterhaltung des Betriebs, wie z. B. Business Continuity Management und Krisenmanagement.

Als „Dachgesetz“ werden sektorübergreifende Ziele festgelegt:



Das KRITIS-Dachgesetz richtet sich an Betreiber kritischer Infrastrukturen, also an Unternehmen und Einrichtungen, die

- essenziell für die Gesamtversorgung sind und
- mehr als 500.000 Personen versorgen.

Diese zählen somit laut KRITIS-Dachgesetz als kritische Anlage.

Ziel ist es, die Resilienz der kritischen Anlagen gegenüber allen denkbaren Gefahren – von Naturkatastrophen über Cyberangriffe bis hin zu menschlichem Versagen – zu stärken („All-Gefahren-Ansatz“).

Die zehn Sektoren:



*Im Gesetz wird der Sektor wörtlich als „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende“ betitelt



Anwendungsbereich für das KRITIS-Dachgesetz

Ist mein Unternehmen auf die kommenden Anforderungen vorbereitet?

Sektorale Zugehörigkeit:

Ist mein Unternehmen einem der **zehn Sektoren des KRITIS-Dachgesetzes** zugehörig?



Systemrelevanz:

Ist mein Unternehmen essenziell für die **Gesamtversorgung** in Deutschland?



Versorgungsrelevanz:

Versorgt mein Unternehmen **mehr als 500.000 Personen**?



Spezifische Schwellenwerte:

Überschreitet mein Unternehmen die **sektorspezifischen Schwellenwerte** der [BSI-Kritisverordnung](#)?



Abhängigkeit von anderen Betreibern:

Ist mein Unternehmen **Teil der Versorgungskette**, auf die andere Betreiber kritischer Anlagen, auch in anderen Sektoren, angewiesen sind?



Bestehende gesetzliche Verpflichtungen:

Bin ich aktuell bereits durch andere Gesetze, wie z. B. [BSI-Gesetz](#) [NIS-2](#) oder [CER-Richtlinie](#) (in einem anderen EU-Land) reguliert?





Anforderungen des KRITIS-Dachgesetzes

Ist mein Unternehmen auf die **kommenden Anforderungen** vorbereitet?

Registrierungspflicht:

Muss mein Unternehmen sich beim **BBK/BSI** als Betreiber kritischer Infrastrukturen registrieren?



Risikoanalyse und Risikobewertung der kDL:

Werden **Risikoanalysen und -bewertungen** hinsichtlich des Kernbetriebs sowie der Verfügbarkeit der kritischen Dienstleistung (kDL) vorgenommen?



Resilienzplanung:

Haben wir einen **Resilienzplan** erstellt, der Risiken, Schutzmaßnahmen und Wiederherstellungsstrategien dokumentiert?



Kontinuierliche Verbesserung:

Verfügen wir über einen Prozess zur **kontinuierlichen Verbesserung**?



Interdependenzen:

Wurden **Maßnahmen** hinsichtlich des Ausfalls von kritischen Dienstleistungen anderer Unternehmen vorgenommen?



Krisenmanagementverfahren:

Haben wir **Krisenmanagementverfahren** implementiert, die klare Rollen, Abläufe und Eskalationsstufen definieren?



All-Gefahren-Ansatz:

Berücksichtigen unsere Analysen **alle denkbaren Risiken** – z. B. Naturgefahren, vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen?



Bauliche, technische und organisatorische Maßnahmen:

Haben wir physische Schutzmaßnahmen wie z. B. **Zugangskontrollen, Videoüberwachung** oder **Detektionsgeräte** im Einsatz?



Aufrechterhaltung des Betriebs:

Sind **Strategien und Maßnahmen** zur Aufrechterhaltung des Betriebs definiert, z.B. Notstromversorgung oder alternative Lieferketten?



Meldepflichten:

Haben wir Prozesse etabliert, um **Vorfälle** unverzüglich nach Kenntnisnahme an zuständigen Behörden zu **melden**?



Kontaktdaten:

René Scheffler

Partner
Lead Risk, Business Continuity &
Resilience Assurance
Köln
E-Mail: rscheffler@deloitte.de

Matthias Max

Senior Manager
Risk, Business Continuity &
Resilience Assurance
Berlin
E-Mail: mmax@deloitte.de

Marcel Gözl

Manager
Risk, Business Continuity &
Resilience Assurance
Stuttgart
E-Mail: margoelz@deloitte.de

Kompetenzzentrum Kritische Infrastrukturen e.V.

EUREF-Campus 1-2
10829 Berlin
Andrej Philippi
E-Mail: InfoKKI-Verein@kki-verein.de
Telefon: 030 - 32 29 32 2999

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Mandanten. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 460.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte-Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 09/2025