

Positionspapier zum Referenten-Entwurf des BMI zum KRITIS Dachgesetz vom 21.12.2023



Die Wirtschaftsvertreter des UP KRITIS begrüßen weiterhin die nationale Implementierung der CER-Richtlinie. Mit diesem Gesetzesvorschlag die CER-Richtlinie umzusetzen und gleichzeitig für Deutschland einen Start für die Regulierung des sektorübergreifenden und sektorspezifischen physischen Schutzes zu finden, ist nun deutlicher zu erkennen (z.B. kleinerer Scope als im NIS2UmsuCG, Themen wie „Komponentenbeschaffung“ sind entfallen). Es sollten jedoch unbedingt bis zur ersten Evaluierung des Gesetzes noch weitere Anpassungen vorgenommen werden, um gemeinsam mit dem Thema zielführend und auch praxisgerecht zu starten und erst danach Verbesserungen anzugehen. Hier bietet es sich dringend an, uns noch mehr an dem erfolgreichen Beispiel zur Einführung des IT-Sicherheitsgesetzes zu orientieren. Um dieses Ziel zu erreichen, weist der UP KRITIS in dieser Stellungnahme auf einige Themen hin, bei denen Verbesserungspotential erkannt wurde.

Übergreifend ist immer noch festzustellen, dass Voraussetzungen noch nicht geschaffen sind, um eine vollständige Bewertung (inhaltlich und monetär) des Gesetzesentwurfes vorzunehmen. Zum Beispiel fehlt die nationale Risikoanalyse bzw. die Kenntnis auf welcher Detailtiefe welche Themenstellungen in dieser adressiert werden und somit auch die zu betrachtende Szenarien für die betrieblichen Risikoanalyse und deren Maßnahmenableitung und Kostenabschätzungen. Auch das die Rechtsverordnung nach § 16 noch nicht vorliegt, erschwert eine Gesamtbeurteilung. Der UP KRITIS trifft die Annahme, dass dieses Gesetz die KRITIS Betreiber betrifft, die mehr oder weniger zur Zeit von der IT-Sicherheitsgesetzgebung betroffen sind (ca. 2.000 Unternehmen). Der UP KRITIS bietet an, gemeinsam steuerbare Risiken und auch betroffene Branchen und kritischen Dienstleistungen zu identifizieren.

Der UP KRITIS bedauert, dass der Kommentierungs-Entwurf zum NIS2UmsuCG immer noch nicht vorliegt, um erkennen zu können, ob diese beiden Gesetze zum Thema nationaler Sicherheit ineinandergreifen, sich ergänzen und nicht doppelt regulieren.

Es gibt keine Angaben zu den Bußgeldhöhen, wodurch hierzu keine detaillierte Betrachtung durch den UP KRITIS erfolgen kann. Den Ansatz, erst zu einem späteren, noch nicht endgültig definierten Zeitpunkt Bußgelder einzuführen, kann der UP KRITIS nachvollziehen, sieht aber Verbesserungspotential.

Der UP KRITIS verzichtet hier auf Formulierungsvorschläge, da diese auch von Branchenverbänden eingereicht werden und versucht mit dieser Stellungnahme das Thema grundsätzlich zu betrachten. Wir übersenden unsere Detail-Hinweise in der angehangenen Tabelle und einen uns wichtigen Vorschlag zur Zeitschiene und Abhängigkeiten insbesondere im Bezug zu Vorgaben und Auswahl geeigneter Schutzmaßnahmen nach §10 (1) mit dieser Stellungnahme zur weiteren Verwendung.

Zur effektiven und kosteneffizienten Erhöhung der sektorübergreifenden physischen Sicherheit, weisen wir auf folgende Verbesserungsmöglichkeiten hin und hoffen auf eine praxistaugliche nationale Umsetzung unter Einbeziehung der Wirtschaft unter anderem auch durch einen Anhörungstermin zu diesem Referentenentwurf.

Themenschwerpunkte

- 1. Berücksichtigung von inhaltlichen und zeitlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz nach Artikel 1, §10 (1)**

Die angehangene „Zeitschiene“ mit den Abhängigkeiten zeigt sehr deutlich, dass die Umsetzung des Gesetzes in der vorliegenden Fassung in der betrieblichen Praxis nicht möglich ist. Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit Ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben.
- 2. Erfüllungsaufwand für die Wirtschaft**

Trotz der noch unklaren konkreten Ausführung zu Betroffenheit von Unternehmen und Detailtiefe, welche Themenstellungen in den Regelungen wie adressiert werden, haben die Wirtschaftsvertreter auf den Erfahrungen des IT-Sicherheitsgesetzes und den bisherigen Gesprächen mit dem BMI zum KRITIS-DachG erste vorsichtige Kostenschätzungen vorgenommen.

Im Verhältnis zu den unter E3 für die Verwaltung mit „erheblichen Erfüllungsaufwand“ bezeichneten Kosten entstehen jedem betroffenen Unternehmen mindestens ein ähnlicher Kostenaufwand, so dass unter E2 zur klaren Information des Gesetzgebers im Minimum ebenfalls von „erheblichem Erfüllungsaufwand für alle betroffene Unternehmen“ zu sprechen ist. In dieser Betrachtung sind noch keine etwaig notwendigen technischen, baulichen Maßnahmen enthalten.
- 3. Zuständigkeiten in der Durchsetzung und Aufsicht**

Im vorliegenden Gesetzesentwurf sind die Behördenzuständigkeiten zum Thema Durchsetzung und Aufsicht nicht eindeutig geregelt bzw. lassen die Vermutung zu, dass betroffene Unternehmen (insb. „Verbundunternehmen“) im Rahmen der Bundes- und Landeshoheit verschiedenen Regelungen z.B. bei der „Nachweiserbringung“ befolgen müssen. Hier ist eine Harmonisierung dringend erforderlich.
- 4. Vermeidung von Mehrfachregulierung: Harmonisierung der gesetzlichen Regelungen**

Wir empfehlen die ausschließliche Regulierung von physikalischen Sicherheitsthemen. Eine Harmonisierung der Gesetzlichen Regelungen bzgl. Begriffsbestimmungen und deren Anwendung ist zwingend erforderlich.
- 5. Identifizierung von betroffenen Unternehmen**

Wir begrüßen, dass im Gesetz die Rahmenbedingungen zur Rechtsverordnung nun festgeschrieben sind. Beteiligung der Wirtschaft bei der Ausgestaltung der Rechtsverordnung ist weiterhin gewünscht.
- 6. Risikobetrachtung**

Es sollte auf die KRITIS-Verordnung referenziert werden und nur die Versorgungssicherheit als Kriterium herangezogen werden. Wir begrüßen die sektorspezifischen nationalen Risikoanalysen. Diese sollten unter Beteiligung der Wirtschaft erstellt werden.

7. Registrierungspflicht, Benennung Kontaktstelle

Es soll ein gemeinsames Online-Portal (bestenfalls gleichzeitig auch als Meldeportal für Störungen und Portal um alle notwendigen Nachweise zu erbringen) für das NIS2UmsuCG und das KRITIS DachG betrieben werden. Aufgrund der Sensibilität der Daten muss dieses Portal besonderen Sicherheitsanforderungen genügen. Hier sollten auch alle zukünftig zuständigen Behörden ihren notwendigen Zugriff erhalten. Diese Daten dürfen nur zum Zwecke der Gefahrenabwehr genutzt werden.

8. Zu ergreifende Maßnahmen

Den Wirtschaftsvertretern des UP KRITIS ist nicht klar, was mit einem „Resilienzplan“ adressiert werden soll. Dies sollte konkretisiert werden. Es sollte darauf hingewiesen werden, dass bereits eine zielführende und praxisgerechte Planung von notwendigen Maßnahmen und deren entsprechende spätere Umsetzung ausreicht, um dem Ziel dieses Gesetzes gerecht zu werden. Bauliche Maßnahmen können Monate/Jahre in Anspruch nehmen.

9. Meldewesen

Es sollte weiterhin der Grundsatz „Ein Vorfall - Eine Meldung“ gelten. Daneben ist anzumerken, dass ein Informationsfluss vom BBK an die Betreiber der kritischen Anlagen weiterhin nicht angedacht ist.

10. Bußgeldvorschriften

Der UP KRITIS schlägt vor, zumindest bis zur ersten regulären Evaluierung des Gesetzes, den Ansatz zur Bußgeldhöhe des IT-SIG 1.0 zu wählen und nicht den des NIS2UmsCG.

Weitere Detailhinweise

1. Berücksichtigung von zeitlichen und inhaltlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz nach Artikel 1 §10 (1)

Die angehangene „Zeitschiene“ mit den Abhängigkeiten zeigt sehr deutlich, dass die Umsetzung des Gesetzes in der vorliegenden Fassung in der betrieblichen Praxis nicht möglich ist. Die dort aufgezeigten Abhängigkeiten machen klar, dass betriebliche Notwendigkeiten bei der Gesamtausgestaltung zu berücksichtigen sind (Risikoidentifizierung, Maßnahmenidentifizierung und -planung, Budgetierung, Ausschreibungsverfahren, Beantragung von etwaigen baulichen Genehmigungen, bis zur Umsetzung). Erschwert wird das Thema in der augenblicklichen Fassung insbesondere durch die fehlende Planungssicherheit, die die angedachten, aber noch nicht existierenden behördlichen Vorgaben zur Ausgestaltung der Resilienzmaßnahmen nach §10 (1) mit sich bringen!

Aus Sicht des UP KRITIS, sollten somit die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), in den Artikel 2 ausgelagert und die Inkraftsetzung in Abhängigkeit zur Evaluierung gesetzt werden. Somit kann später deren Notwendigkeit im Rahmen der Evaluierung des Gesetzes geprüft werden. Dieses ist zurzeit schon für die sektorspezifischen Rechtsverordnungen der Länder so vorgesehen und sollte auf Bundesvorgaben ausgeweitet werden. Somit würde das Thema der Ausgestaltung des §10 (1) für die Länder und den Bund in der ersten Fassung gleichbehandelt werden und dort keinen bis kaum Aufwand erzeugen.

Die Einführung des IT-Sicherheitsgesetzes hat nachweislich gezeigt, dass die Wirtschaft mit ihren Branchenverbänden auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse (branchenspezifischen Sicherheitsstandards) etablieren konnte. Bis auf die Rechtsverordnung zur Bestimmung von KRITIS-Betreibern nach BSI-KRITIS VO wurde im Rahmen der Einführung des IT-Sicherheitsgesetzes auf die Nutzung dieses Rechtsmittels zur Vorgabe von Maßnahmen in den letzten 8 Jahren verzichtet und wir konnten im europäischen Vergleich in Deutschland ein sehr hohes Sicherheitsniveau erreichen. Es ist zusätzlich davon auszugehen, dass die zukünftig betroffenen Unternehmen auch schon heute, u.a. aufgrund von bereits existierenden rechtlichen Rahmenbedingungen (aus IT-SIG oder UVV, etc.), insbesondere, auch im eigenen Interesse und nach Risikoabwägungen, ein geeignetes Maß an physischen Maßnahmen etabliert haben.

Es kann auf weitere Vorgaben zu Resilienzmaßnahmen von behördlicher Seite aus Sicht des UP KRITIS auch verzichtet werden, da mit den in §10 (6) angedachten zu entwickelnden branchenspezifischen Mindeststandards, unter Berücksichtigung der „Leitplanken“ aus §10 (1) und (3) ein praxisnaher und vor allem risikobasierter Ansatz ermöglicht würde.

Sollte das Instrument der Rechtsverordnung trotz unserer dringenden Empfehlung weiter angedacht sein, ist die Wirtschaft mit ihren Branchenverbänden zwingend in deren Erstellung einzubeziehen, damit deren Erfahrung hier einfließen kann und praxistaugliche Vorgaben zur Ausgestaltung des §10 (1) entstehen können. Zudem sollte dieser Eingriff das letzte Mittel der Wahl sein. Des Weiteren ist auf der Zeitachse diese Einflussnahme in die betrieblichen Abläufe zu berücksichtigen und angemessene Umsetzungsfristen zur Berücksichtigung dieser Vorgaben vorzusehen. Dieses kann bei baulichen Maßnahmen sehr schnell mehrere Jahre in Anspruch nehmen.

2. Vermeidung von Mehrfachregulierung: Harmonisierung der Gesetzlichen Regelungen

Hierzu müssen Begrifflichkeiten in allen deutschen Gesetzen einheitlich gewählt und genutzt und nicht doppelt definiert werden. Eindeutige, einheitliche und konsistente Verwendung ist hier zwingend erforderlich. Doppelung von Pflichten (z.B. Registrierungs-, Nachweis- und Meldepflichten sowie die Umsetzung von Maßnahmen) aus den unterschiedlichsten nationalen Gesetzen wie dem BSIG, EnWG, TKG,

KRITIS DachG usw. und europäischen Regulierungsvorgaben müssen vermieden werden. Zudem dürfen spezialrechtliche Normen und Bescheide von Fachbehörden sowie deren Zweckmäßigkeit durch das BBK nicht in Frage gestellt werden.

Eine Doppelung von Bußgeldern für den gleichen Sachverhalt muss ausgeschlossen sein.

Da das NISUmsuCG noch nicht vorliegt, besteht hier die große Gefahr, dass die Bestimmungen der Gesetze auseinanderlaufen und die Betreiber/Unternehmen hier in naher Zukunft bei der Umsetzung Probleme bekommen.

Die Behördenzuständigkeit muss klar geregelt und für die Wirtschaft erkennbar sein. Auch hier dürfen keine sich überschneidenden Zuständigkeiten geschaffen werden und die zuständige Behörde muss in die Lage versetzt werden diesen Pflichten nachzukommen. Nicht zuletzt, damit behördliche Prozesse, von denen die Betreiber abhängen, auch frist- und sachgerecht abgearbeitet werden können (z.B. nationale Risikoanalyse).

Für Unternehmen, die zukünftig sowohl nach NISUmsuCG als auch nach KRITIS DachG den Nachweispflichten unterliegen, muss eine Behörde mit der Aufgabe der Gesamtkoordination benannt werden, welche bei etwaigen Überschneidungen, die sich ggf. auch bei sehr guter gesetzlicher Regelung der Zuständigkeiten nicht vollständig vermeiden lassen, eine für alle Seiten bindende Entscheidung treffen darf. Die Erbringung von Nachweisen durch Audits muss in Form von „Gesamtaudits“ für Anforderungen nach NISUmsuCG und nach KRITIS DachG möglich sein.

3. Identifizierung von betroffenen Unternehmen

Die Wirtschaftsvertreter des UP KRITIS sehen bei der Identifizierung von kritischen Anlagen auch die Notwendigkeit die öffentliche Bundesverwaltung, insbesondere rund um die öffentliche Sicherheit, mit einzubeziehen (auch hier sollten der gleiche Maßstab angesetzt werden, wenn eine Bundesverwaltung für mehr als 500.000 Mitbürger zuständig ist, sollte diese im Scope des Gesetzes sein). Des Weiteren sind die Betreiber kritischer Anlagen im Falle einer großflächigen Krise, welche durch das BBK koordiniert werden soll, auch von dem BBK abhängig. Für solche Fälle muss das BBK auch in die Lage versetzt werden dieser Verpflichtung nachzukommen und nicht selbst durch sicherheitstechnische Probleme handlungsunfähig sein. Somit sieht der UP KRITIS den § 17 (Ausnahmebescheid) als sehr kritisch an.

4. Risikobetrachtung

Regelungsinhalte wie "oder andere dramatische Folgen eintreten würden" oder "erhebliche Störungen der wirtschaftlichen Tätigkeit" sind nicht eindeutig (jedes Unternehmen wird darunter was anderes verstehen). Bisher wurde die Versorgungssicherheit adressiert. Hier fehlen die Kriterien wann etwas erheblich oder dramatisch ist.

Wir begrüßen, dass auf betrieblicher Ebene die Wirtschaftlichkeit bei der Auswahl der Maßnahmen mitberücksichtigt wird. Dies sollte nicht nur in der Gesetzesbegründung, sondern auch im Gesetzestext vermerkt sein. Die Wirtschaftlichkeit ist die Voraussetzung, dass ein Unternehmen eine Dienstleistung anbietet.

Wir begrüßen die sektorspezifischen nationalen Risikoanalysen, um die Besonderheiten des jeweiligen Sektors berücksichtigen zu können. Bei den nationalen Risikoanalysen und -bewertungen sollten die Wirtschaftsverbände beteiligt werden, um die behördliche Sicht mit den Praxiserfahrungen zu spiegeln und sektor- und branchenspezifische Risiken zu ergänzen. Dieses wird auch von der CER-Richtlinie vorgesehen.

Bestimmte durch die nationalen Risikoanalysen und -bewertungen identifizierte Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) können durch die Betreiber kritischer Anlagen in ihren Resilienzplänen nur bedingt berücksichtigt werden. In diesen Fällen sollten Bund und Länder auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) die Betreiber kritischer Anlagen bzw. die kritischen Anlagen angemessen schützen.

Problematik: Berücksichtigung von Abhängigkeiten bei den betrieblichen Risikoanalysen. Im Energiesektor z.B. würden die Risiken ins unendliche reichen (Blackout Kaskadeneffekt auf Europa)! Beim ITSIG wurden diese Effekte mit gutem Grund ausgeblendet, da sonst keine wirtschaftliche Betrachtung der Risiken und der zu ergreifenden Maßnahmen möglich sind. Sicherheitsmaßnahmen müssen für die betroffenen Unternehmen wirtschaftlich vertretbar sein.

Die Risikobetrachtung ist bisher sehr statisch. Es muss die Möglichkeit bestehen, Anpassungen an aktuelle Risikolagen vorzunehmen und unbürokratisch Maßnahmen zu implementieren. Ein Hinweis, das auch abweichend von dem Risiko-Life-Cycle relevante kritische Sachverhalte geeignet Berücksichtigung finden sollten, sind mit aufzunehmen.

5. Zeitliche Abfolge

Die angedachten Stichtage und Zeiträume bei der Implementierung des Gesetzes müssen zwingend überarbeitet werden (siehe mitgelieferte „Zeitschiene“). Zum Beispiel können die betrieblichen Risikoanalysen erst nach den nationalen Risikoanalysen durchgeführt werden. Dann braucht es die Resilienzstandards, um geeignete Maßnahmen zu identifizieren, die diesen Risiken entgegenwirken. Im Anschluss müssen diese Maßnahmen implementiert werden. Dieser Zusammenhang muss durch den Gesetzgeber berücksichtigt werden.

Die übermittelte „Zeitschiene“ lässt klar erkennen, dass es hier noch einer Justierung bedarf. Der UP KRITIS hat einen ersten Vorschlag erarbeitet (Siehe Anlage KRITIS-DachG-Vers1.xls „Vorschlag „Timeline““), um hier eine praxistaugliche Umsetzung zu gewährleisten und steht für einen intensiveren Austausch zu dem Thema zur Verfügung.

6. Registrierungspflicht, Benennung Kontaktstelle

Es soll ein gemeinsames Online-Portal (bestenfalls gleichzeitig auch als Meldeportal für Störungen und Portal um alle notwendigen Nachweise zu erbringen) für das NIS2UmsuCG und das KRITIS DachG betrieben werden. Hierbei muss sichergestellt werden, das Unternehmen auch in geeigneter Art und Weise Daten einpflegen können (z.B. nicht nur Online in „Echtzeit“, sondern auch vorbereitend die notwendigen Datenabfragen zur Verfügung gestellt werden). Da es sich um sehr sensible Daten handelt, muss dieses Portal IT-technisch sicher betrieben und den betroffenen Unternehmen ein geeigneter Zugang eingerichtet werden. Listen, die das BBK aus diesem Portal entnimmt (z.B. Liste aller Betreiber kritischer Anlagen) müssen vertraulich (Vertraulichkeit, Geheimhaltung) behandelt werden und dürfen nicht veröffentlicht werden und zweckgebunden sein. Das BBK/BSI muss entsprechende Schutzmaßnahmen ergreifen, um die Vertraulichkeit zu gewährleisten.

Auf Unternehmensseite sollte keine Personen als Kontakt definiert werden können, sondern Funktionen (24/7 Erreichbarkeit).

7. Zu ergreifende Maßnahmen

Hier wird bei zukünftig zu implementierenden Maßnahmen auch auf den Stand der Technik verwiesen, somit u.a. die zukünftigen branchenspezifischen Resilienzstandards. Hierbei ist zwingend ein Bestandsschutz der bereits etablierten Sicherheitsmaßnahmen unter dem Aspekt der Wirtschaftlichkeit und Funktionalität zu berücksichtigen. In der Regel ist es Betreibern nicht möglich, zeitnah großflächig Sicherheitsinfrastruktur auszutauschen.

Den Wirtschaftsvertretern des UP KRITIS ist nicht klar, was mit einem „Resilienzplan“ adressiert ist. Sind damit,

- a) Maßnahmen die bereits implementiert sind, oder

- b) ergänzende und neue Maßnahmen die zukünftig implementiert werden sollen, da noch Maßnahmen fehlen, oder
- c) Beides (a) und b)) adressiert.

Wichtig hierbei ist, dass die Identifizierung und angemessene zeitliche Planung von notwendigen Maßnahmen (unter Berücksichtigung der betrieblichen Praxis wie z.B. die Budgetplanung, Ausschreibungsprozesse/-fristen, Einholung von Baugenehmigungen, etc...) als ausreichende Erfüllung der Anforderungen anerkannt werden muss.

Die gewählte Detailtiefe in den Resilienzplänen, die evtl. der zuständigen Behörde als Nachweis zur Verfügung gestellt werden müssen (inklusive Informationen aus der Risikoanalyse, die zu der Auswahl der Maßnahme führten), sind für Maßnahmenpläne weder praxisüblich noch notwendig. Die anforderungsgemäß enthaltenen Informationen können je nach Detailtiefe äußerst sensibel sein.

8. Meldewesen

Auch hier verweisen wir auf das zentrale Portal, welches auch als „Meldeportal“ fungieren soll.

Neben den Meldungen im dem zentralen Meldeportal an das BBK/BSI, welche bei Bedarf an die BNetzA (auch für Meldeprozesse, die es diesbezüglich in Richtung Versorgungssicherheit schon gibt, z.B., EnWG §52), dem BKA oder dem Verfassungsschutz weitergegeben werden, wäre es wünschenswert auch weitere behördliche Meldeprozesse bei Sicherheitsvorfällen hierüber zu unterstützen (z.B. Datenschutzbehörden, sonstige Aufsichtsbehörden). Im Finanzsektor ist dieses durch DORA bereits umgesetzt.

Ein Vorfall - Eine Meldung!

Es fehlt ein Informationsfluss vom BBK an die Betreiber der kritischen Anlagen. Hier müssen zeitnah Warnungen über nationale/europäische physikalische Störungen/Bedrohungen/Risiken vom BBK an die Betreiber fließen. Dieses ist auch im BSIG bzw. NIS2UmsuCG so geregelt und hilft den Betreibern sich gegen dolose Handlungen zu schützen, bzw. diese bei Ihren Risikobetrachtungen zu berücksichtigen.

9. Bußgeldvorschriften

Der UP KRITIS schlägt vor, zumindest bis zur ersten regulären Evaluierung des Gesetzes, den Ansatz zur Bußgeldhöhe des IT-SIG 1.0 zu wählen und nicht den des NIS2UmsuCG. Die maßnahmenbezogenen Bußgeldvorschriften erst einzuführen, nachdem es branchenspezifische Resilienzstandards gibt, scheint dem UP KRITIS zielführend. Hier muss jedoch eine Umsetzungsfrist eingeplant werden, damit diese Standards bei Risikoanalysen, Maßnahmenplanungen und -umsetzungen berücksichtigt werden können.

10. Besondere Behandlung von Betreibern kritischer Anlagen

Mit diesem Gesetz sollte klar definiert werden, dass Kritische Infrastrukturen einen besonderen Status bei der Bewertung von Vorfällen haben. Z.B. bei einer Pandemie müssen trotz Ausgangssperren, Mitarbeiter von Betreibern kritischer Anlagen noch Zutritt zu den Anlagen ermöglicht werden. Bei Hochwassersituationen sollten Betreiber kritischer Anlagen bevorzugt unterstützt werden, damit die Kritische Infrastruktur vorrangig wieder in Betrieb genommen werden kann bzw. geschützt bleibt.

Bei Verwaltungsentscheidung sollten Maßnahmen zur Steigerung der notwendigen Resilienz bei Betreibern von kritischen Anlagen mit besonderem Gewicht berücksichtigt werden (z.B. Sicherheit vor Denkmalschutz oder Sicherheit vor Transparenzpflichten).

11. Personalüberprüfung

Zurzeit sind personelle Sicherheitsüberprüfungen nur sehr eingeschränkt möglich (außer Telekommunikation/ÜNB/teilweise VNB). Nur die Nutzung von Terrorlisten/Sanktionslisten bei

Bestandspersonal und polizeiliche Führungszeugnisse bei Einstellung sind Möglichkeiten, das Thema abzudecken.

Unternehmen sollte die Möglichkeit eingeräumt werden, Personal mit sicherheitskritischen Aufgaben zu überprüfen/überprüfen zu lassen bzw. in die Lage zu versetzen, sich mit Sicherheitsbehörden auszutauschen. Hierzu sollte der Staat in diesem Gesetz eine Grundlage für Unternehmen schaffen. Ohne gesetzliche Grundlage sind „Überprüfungsmaßnahmen“ nach DSGVO untersagt.

Gleichzeitig unterstützen wir, dass entsprechende bereits existierende Vorschriften über Zuverlässigkeitsüberprüfungen unberührt bleiben.

12. Evaluierung

Wenn wir den Gesamtzeitablauf sehen, scheinen 5 Jahre für eine Evaluierung angemessen, insbesondere wenn zu diesem Zeitpunkt über die Notwendigkeit der Einführung zu weiteren Vorgaben bzgl. implementierender Maßnahmen entschieden werden soll. Es sollte jederzeit die Möglichkeit bestehen auf veränderte Sicherheitslagen unter Einbeziehung der Wirtschaft zu reagieren. Hiermit soll sichergestellt werden, dass die Auswirkungen auf die Wirtschaft berücksichtigt werden und für die Betreiber der Kritischen Anlagen Planungssicherheit gegeben ist.

Zum regulären Evaluierungszeitpunkt können auch die Kosten der Umsetzung (einmalig und fortlaufend (CAPEX/OPEX) benannt werden. Wir empfehlen eine zentrale Abfrage über das Bundesamt für Statistik.

13. Inkrafttreten

Der UP KRITIS schlägt dringend vor, §10 (4) und (5) des Artikel 1 in den Artikel 2 zu überführen. Hier ist auch das Thema der sektorspezifischen Rechtsverordnungen zur Ausgestaltung des §10 (1) angesiedelt. Beide Absätze sollten im Artikel 3 erst nach der Evaluierung des Gesetzes (2029/30) in Kraft gesetzt werden. Zu diesem Zeitpunkt kann geprüft werden, ob diese Verordnungen und Mindeststandards notwendig sind, um das Ziel zu erreichen und etwaige zusätzliche Regelungen können in der betrieblichen Praxis im Risiko-Life-Cycle berücksichtigt werden.

		Gesetzestext	Kommentar: TAK Regulierung konsolidiert
Referentenentwurf			
Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen			
A		Problem und Ziel <p>Am 16. Januar 2023 trat die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164; sog. CER-Richtlinie) in Kraft. In der mit der Richtlinie (EU) 2022/2557 aufgehobenen Richtlinie 2008/114/EG des Rates (ER-Richtlinie) war lediglich ein Verfahren für die Ausweisung europäischer kritischer Infrastrukturen im Energiesektor und im Verkehrssektor vorgesehen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen in mindestens zwei Mitgliedstaaten hätte. Mit der Richtlinie (EU) 2022/2557 wurde ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen in mindestens elf Sektoren gegen Gefahren auch außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen. Ziel der Richtlinie ist es, einheitliche Mindestverpflichtungen für kritische Einrichtungen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmassnahmen zu garantieren. Um die Resilienz dieser kritischen Einrichtungen, die für das reibungslose Funktionieren des Binnenmarktes von entscheidender Bedeutung sind, zu stärken, schafft die Richtlinie (EU) 2022/2557 einen übergreifenden Rahmen („Dach“), der im Sinne des All-Gefahren-Ansatzes Naturkatastrophen oder vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen berücksichtigt. Die Richtlinie (EU) 2022/2557 ist gemäß ihrem Artikel 26 Absatz 1 bis zum 17. Oktober 2024 in nationales Recht umzusetzen.</p> <p>Der Schutz der IT-Sicherheit von kritischen Infrastrukturen ist bereits im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSiG) niedergelegt. Durch die Umsetzung der NIS-2-Richtlinie (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsoG) und durch die DORA-Verordnung werden die Regelungen für den Schutz der IT-Sicherheit kritischer Anlagen und weiteren Einrichtungen weiterentwickelt. Das KRITIS-DachG wird für die Resilienz von Betreibern kritischer Anlagen nach dem „All-Gefahrenansatz“ (im Folgenden zur Abgrenzung von der IT-Sicherheit technisch „physischer Schutz“) neben diese Regelungen treten, aber gleichzeitig eine größtmögliche Kohärenz vorsehen, indem die Schnittstellen zwischen den Bereichen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend ausgestaltet werden.</p> <p>Zu beachten ist dabei, dass bei der Umsetzung der NIS-2-Richtlinie das bereits umfassend bestehende Regelungswerk zum Schutz der IT-Sicherheit erweitert wird, während im Hinblick auf die physischen Resilienzmaßnahmen dieses Gesetzes mit der Umsetzung der Richtlinie (EU) 2022/2557 erstmals eigenständige und sektorenübergreifende Regelungen getroffen werden. Daher ist der Anwendungsbereich des KRITIS-DachG kleiner und die Regelungsintensität geringer als bei den Regelungen zur Umsetzung der NIS-2-Richtlinie. Durch gestufte Anforderungen an Betreiber kritischer Anlagen und wichtige und besonders wichtige Einrichtungen im KRITIS-DachG und im BSI-G wird damit auch den Belangen der Wirtschaft Rechnung getragen.</p> <p>Das KRITIS-DachG wird keine sektoren- oder gar branchenspezifischen Regelungen treffen, sondern abstrakt vorgeben, dass in allen KRITIS-Sektoren geeignete und verhältnismäßige Maßnahmen zum physischen Schutz von Betreibern kritischer Anlagen zu treffen sind. Dazu setzt das KRITIS-DachG einen Prozess auf, der insbesondere nationale und betriebsseitige Risikobewertungen in allen Sektoren, die Erstellung von Resilienzplänen durch die Betreiber, die Erarbeitung branchenspezifischer Schutzstandards durch die Verbände und Äquivalenzprüfungen durch fachlich zuständige Behörden in den verschiedenen Sektoren beinhaltet.</p>	<p>„Besonders wichtige“ und „wichtige Einrichtungen“ auch im KRITIS DachG? => NEIN!</p> <p>Eindeutige Klarstellung, dass diese nur in der neuen KRITIS-VO benannt werden, da diese Definitionen für die Umsetzung der NIS2 Richtlinie im NIS2UmsoG benötigt werden und sich das NIS2UmsoG zukünftig auch auf die neue KRITIS-VO beziehen wird, sobald diese in Kraft gesetzt wurde (ab dem 17.07.2026).</p> <p>Bis dahin bezieht sich das NIS2UmsoG auf die bestehende BSI-KRITIS-VO!</p> <p>In § 9 KRITIS Dachgesetz wird das auch klar aufgezeigt!</p>
B		Lösung <p>Die europarechtlichen Vorgaben der Richtlinie (EU) 2022/2557 werden mit dem vorliegenden neuen Stammgesetz umgesetzt. Es enthält Regelungen zur Identifizierung kritischer Anlagen, die in einer Verordnung weiter konkretisiert werden, sowie für deren Registrierung. Betreiber kritischer Anlagen, die kritische Dienstleistungen in oder für mindestens sechs Mitgliedstaaten betreiben, werden als kritische Einrichtungen von besonderer Bedeutung für Europa identifiziert und unterliegen besonderen Maßnahmen. Den Betreibern kritischer Anlagen werden Maßnahmen auferlegt, die ihre Resilienz stärken sollen. Dazu gehört die Erarbeitung und Umsetzung von Resilienzplänen, in denen auf der Basis von Risikoanalysen und Risikobewertungen der kritischen Einrichtung dargestellt wird, welche geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Stärkung der Resilienz getroffen werden. Das KRITIS-DachG enthält Resilienzziele, die die Betreiber kritischer Anlagen mit ihren Maßnahmen erreichen müssen sowie zur Orientierung eine Übersicht von beispielhaften Maßnahmen, die sie treffen könne. Zur weiteren Konkretisierung von sektorenübergreifenden Resilienzmaßnahmen wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe einen Katalog mit Mindestanforderungen erarbeiten. Um auch sektorspezifische und bundeseinheitliche Resilienzmaßnahmen festzulegen, sieht das KRITIS-DachG ein strukturiertes Verfahren vor. Die Bundesressorts werden ermächtigt, für die in ihrer Zuständigkeit liegenden Bereiche, Rechtsverordnungen zur Konkretisierung der Resilienzmaßnahmen zu erlassen. Angelehnt an die Erarbeitung und Anerkennung von branchenspezifischen Sicherheitsstandards bei der IT-Sicherheit (B35), können darüber hinaus die Betreiber kritischer Anlagen und ihre Branchenverbände branchenspezifische Resilienzstandards entwickeln und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe diese als die Anforderungen des KRITIS-DachG erfüllend anerkennen. Solange und soweit es keine entsprechenden branchenspezifischen Resilienzstandards gibt, werden auch die Landesregierungen ermächtigt, Rechtsverordnungen zur Konkretisierung der Resilienzmaßnahmen für die in ihrer Zuständigkeit liegenden Bereiche zu erlassen. Darüber hinaus müssen Betreiber kritischer Anlagen eine Kontaktstelle benennen und erhebliche Störungen an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mittels einer gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik eingerichteten digitalen Plattform melden. So soll es für Meldungen nach dem KRITIS-DachG und nach dem BSiG nur eine Meldung durch die Betreiber kritischer Anlagen geben müssen. Mittels der eingegangenen Meldungen über erhebliche Störungen sollen weitere Betreiber kritischer Anlagen gewarnt und durch Informationsaustausch mit anderen Behörden, die sich mit der Resilienz kritischer Infrastrukturen befassen, soll das Gesamtsystem zielgerichtet verbessert werden. Um einen Gesamtüberblick über die Risiken für kritische Dienstleistungen zu erhalten und die Betreiber kritischer Anlagen bei ihren Maßnahmen zu unterstützen, werden regelmäßig nationale Risikoanalysen und Risikobewertungen für die kritischen Dienstleistungen durchgeführt. Das Gesetz enthält keine Entscheidungen über Ressourcenverteilungen.</p> <p>Das KRITIS-DachG wird somit im Hinblick auf nicht-IT-bezogene Maßnahmen zur Stärkung der Resilienz der Betreiber kritischer Anlagen erstmals einheitliche bundeseinheitliche sektorenübergreifende Mindestvorgaben normieren.</p> <p>Beim KRITIS-DachG und der damit verbundenen Umsetzung der Richtlinie (EU) 2022/2557 sowie bei der Umsetzung der NIS-2-Richtlinie durch das entsprechende Umsetzungsgesetz werden die Schnittstellen zwischen den Bereichen IT-Sicherheit und physischen Resilienzmaßnahmen von Betreibern kritischer Anlagen berücksichtigt und Regelungen angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend ausgestaltet. Die im KRITIS-DachG</p>	<p>BBK erarbeitet Mindestandards, Bundesbehörden (z.B. BNetzA) können Rechtsverordnungen zu sektorenübergreifenden und sektorspezifischen Resilienzmaßnahmen und Verbände branchenspezifische Resilienzstandards erstellen.</p> <p>Ohne branchenspezifische Resilienzmaßnahmen können Landesregierungen sektorspezifische Rechtsverordnungen erlassen (werden diese dann durch B35 wieder hinfällig?)</p> <p>Sollten sektorenübergreifenden und sektorspezifischen Resilienzmaßnahmen von Seiten der Behörden, entgegen unserer Empfehlung, vorgegeben werden, müssen diese im "Wording" und auch inhaltlich harmonisiert werden. Frage: Wer wird die zu prüfende Stelle sein, die diese Vorgaben ggfls. überprüft, harmonisiert? Im TK-Bereich mit Zuständigkeit BNetzA ist es das BSI. Diese Zuständigkeiten sollen auch im KRITISDachG mit aufgenommen werden.</p>
C.		Alternativen <p>keine.</p>	
D.		Haushaltsausgaben ohne Erfüllungsaufwand <p>Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen ist finanziell und stellenmäßig im Gesamthaushalt auszugleichen.</p>	
E.		Erfüllungsaufwand	
E.1.		Erfüllungsaufwand für Bürgerinnen und Bürger <p>Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger. Veränderung des jährlichen Zeitaufwands (in Stunden):0 Veränderung des jährlichen Sachaufwands (in Tsd. Euro):0 Einmaliger Zeitaufwand (in Stunden):0 Einmaliger Sachaufwand (in Tsd. Euro):0</p>	Am Ende bezahlen die Kunden/Bürger die Aufwände über Preise oder Steuern
E.2.		Erfüllungsaufwand für die Wirtschaft <p>Durch die Vorgaben des Regelungsentwurfs entsteht der Wirtschaft ein Erfüllungsaufwand. Eine belastbare Schätzung wird erst möglich sein, wenn durch die zugehörigen Rechtsverordnungen der Anwendungsbereich und sektorspezifischen Mindestanforderungen konkret bestimmt werden. Veränderung des jährlichen Erfüllungsaufwands (in Tsd. Euro):tbc davon Bürokratiekosten aus Informationspflichten (in Tsd. Euro):tbc Einmaliger Erfüllungsaufwand (in Tsd. Euro):tbc davon Anschaffung oder Nachrüstung von Maschinen, Anlagen, Gebäuden und Infrastruktureinrichtungen (in Tsd. Euro): tbc davon Einmalige Informationspflicht (in Tsd. Euro):tbc</p>	<p>Weiter unten wird die Annahme getätigt, dass es bei der Wirtschaft einen Erfüllungsaufwand von mehr als 1 Mio. Euro geben könnte.</p> <p>Für die Wirtschaft gilt z.Zt. die Annahme, dass in etwa so viele Wirtschaftsunternehmen betroffen sein werden, wie auch heute auf Basis von IT-SiG 2.0 - geschätzt ca. 2.000 Unternehmen. Bei einer Million Euro in Summe wären das ca. 500 Euro pro Unternehmen! Im Minimum sehen wir eine Größenordnung von 100 Mio. Euro (50 TE je Unternehmen) für die Bürokratie (Feststellung der Betroffenheit, durchzuführende Risikoanalysen, Einrichtung und Bedienung von Meldeprozessen, Auflisten von Resilienzplänen, Bedienung von Nachweispflichten basierend auf Erfahrungen der Umsetzung des IT-SiG). Dazu kommen noch die materiellen Kosten zur Etablierung von zusätzlichen physikalischen Sicherheitsmaßnahmen, welche diesen Wert schnell um ein Vielfaches übersteigen können. Je nach zu berücksichtigendem Risikozuszenario (Stichwort hier: Vorgabe aus nationaler Risikoanalyse) entstehen hier nach unserer Auffassung weitere Aufwände für die Erstimplimentierung im einstelligen Euro Milliardenbereich auf der Wirtschaftseite.</p> <p>Wichtig ist hier festzustellen, dass noch keine konkrete Zahlen genannt werden (können) - auch von dem Hintergrund dass wir intern aufgefordert werden, im Rahmen von Risikoanalysen entsprechende Zahlen zu nennen bzw. zu schätzen.</p>
E.3.		Erfüllungsaufwand der Verwaltung <p>Der Verwaltung entsteht erheblicher Erfüllungsaufwand. Eine belastbare Schätzung für viele Vorgaben wird erst möglich sein, wenn durch die zugehörigen Rechtsverordnungen der Anwendungsbereich und sektorspezifischen Mindestanforderungen konkret bestimmt werden. Aus Vorgaben, die unabhängig der Konkretisierungen der Rechtsverordnungen sind, entsteht der Verwaltung jährlicher Erfüllungsaufwand von rund 6,4 Millionen Euro, davon entfallen 4,3 Millionen Euro auf den Bund und 2,1 Millionen Euro auf die Länder. Zudem entsteht der Verwaltung aus diesen Vorgaben einmaliger Erfüllungsaufwand von rund sechs Millionen Euro, davon entfallen 5,4 Millionen Euro auf den Bund und rund 520 000 Euro auf die Länder. Veränderung des jährlichen Erfüllungsaufwands (in Tsd. Euro):6 379 davon auf Bundesebene (in Tsd. Euro):4 277 davon auf Landesebene (in Tsd. Euro):2 102 Einmaliger Erfüllungsaufwand (in Tsd. Euro):5 970 davon auf Bundesebene (in Tsd. Euro):5 450 davon auf Landesebene (in Tsd. Euro):520</p>	<p>Wenn die Verwaltung schon einen einmaligen und jährlichen Erfüllungsaufwand von jeweils 6 Mio hat, dann wird der Erfüllungsaufwand für die Wirtschaft um ein VIELFACHES mehr! Details haben wir zu E.2 dargestellt.</p> <p>Hinweise: Die fachliche Zusammenarbeit mit den Behörden ist in den letzten Jahren immer besser geworden, allerdings stellt sich bereits heute dar, dass zu viele Planstellen unbesetzt sind und die Kooperation hierunter leidet.</p>
F.		Weitere Kosten <p>Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und das Verbraucherpreisniveau sind nicht zu erwarten.</p>	Es ist zu erwarten, dass die zusätzliche Kosten an den Endverbraucher weiter gegeben werden (Siehe auch E.1)
		Referentenentwurf des Bundesministeriums des Innern und für Heimat	
		Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen) Vom [...] Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:-	
		Artikel 1 Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)	

§1	<p>Nationale KRITIS-Resilienzstrategie</p> <p>Bis zum 17. Januar 2026 verabschiedet die Bundesregierung eine Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen</p>	<p>Es wäre hilfreich, wenn die Strategie vor dem Gesetz zur Verfügung steht.</p> <p>Wenn die Ergebnisse der nationalen Risikoanalyse bei der staatlichen Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen berücksichtigt wird, scheint der Ansatz aus unserer Sicht trotzdem geeignet und sollte auch so mit in den Gesetzestext aufgenommen werden.</p>
§2	<p>Begriffsbestimmungen</p> <p>Im Sinne dieses Gesetzes ist</p> <p>1. „Betreiber kritischer Anlagen“ eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt;</p> <p>2. „Anlage“ eine Betriebsstätte, sonstige ortsfeste Installation, Maschine, Gerät und sonstige ortsveränderliche technische Installation;</p> <p>3. „kritische Anlage“ eine Anlage, die eine kritische Dienstleistung erbringt; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 4;</p> <p>4. „kritische Dienstleistung“ eine Dienstleistung, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, da durch ihren Ausfall oder ihre Beeinträchtigung langfristige Versorgungsengpässe oder Gefährdungen für wirtschaftliche Tätigkeiten, die öffentliche Sicherheit oder Ordnung, die öffentliche Gesundheit, wichtige gesellschaftliche Funktionen oder die Erhaltung der Umwelt eintreten;</p> <p>5. „Resilienz“ die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;</p> <p>6. „Risiko“ das Potenzial für Beeinträchtigungen oder Störungen, die durch einen Vorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Vorfalls zum Ausdruck gebracht wird;</p> <p>7. „Risikoanalyse“ das systematische Verfahren zur Bestimmung des Risikos;</p> <p>8. „Risikobewertung“ der Prozess des Vergleichs und der Priorisierung von Risiken in Bezug auf deren Wirkung auf die kritische Dienstleistung und das Treffen von Entscheidungen hinsichtlich der Notwendigkeit von geänderten oder zusätzlichen Maßnahmen zur Risikobehandlung;</p> <p>9. „Vorfall“ ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich stört oder stören könnte.</p>	<p>Zwingend mit der Begriffsbestimmungen des NIS2-UmsCG abgleichen!</p> <p>Abgleich mit Begriffsbestimmungen Diskussionspapier NIS2-UmsCG:</p> <p>„Betreiber kritischer Anlagen“ ist gleich;</p> <p>„Anlage“ stimmt inhaltlich mit „physischen“ Anlagen nach § 1 Nr. 1 a) & b) BSI-KritisV überein (exkl. c) „Software und IT-Dienste“)</p> <p>„kritische Anlage“ und „kritische Dienstleistung“ wurden in diesem Ref.-E des KRITIS-DG getrennt, dies scheint der Trennung in „kritische Infrastrukturen“ und „wesentlicher Dienst“ in der CER-Richtlinie (EU 2022/2557) zu entsprechen.</p> <p>Die Definition „kritischer Anlagen“ und „kritische Dienstleistung“ wurde jedoch gg.über NIS-2-UmsCG (und KRITIS-VO) genauer bestimmt und ausgeweitet:</p> <p>Im Vergleich zum NIS-2-UmsCG wird statt auf „erhebliche Versorgungsengpässe oder Gefährdungen“ auf „langfristige Versorgungsengpässe oder Gefährdungen“ abgestellt.</p> <p>Das NIS2-UmsCG referiert außerdem abstrakt auf „erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit. (Vgl. „kritische Anlagen [...] die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“)</p> <p>Dem gegenüber bezieht das KRITIS-DG potenzielle „langfristige Versorgungsengpässe oder Gefährdungen“ auf „wirtschaftliche Tätigkeiten, die öffentliche Sicherheit oder Ordnung, die öffentliche Gesundheit, wichtige gesellschaftliche Funktionen oder die Erhaltung der Umwelt“. Dies entspricht den (neuen) Faktoren aus der CER—Richtlinie, kann aber vor allem auch in Verbindung mit §4 des KRITIS-DG als Ausweitung betrachtet werden.</p> <p>Es kann jedoch angezweifelt werden, ob diese Ausweitung im Rechtstext selbst notwendig ist, da in der deutschen Umsetzungsgesetzgebung ohnehin eine klar ausdifferenzierte Ausgestaltung in den nachfolgenden Rechtsverordnungen erfolgt. Die entsprechenden Begriffsbestimmungen des KRITIS-DG sollte daher den Begriffsbestimmungen des NIS2-UmsCG angeglichen werden.</p> <p>Im Besonderen muss aber darauf geachtet werden dass die Ausgestaltung von „kritischen Anlagen“ und „kritischen Dienstleistungen“ in der Rechts-VO entsprechend § 16 KRITIS-DG identisch mit der Ausgestaltung</p>
§3	<p>Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit</p> <p>(1) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe ist zentrale Anlaufstelle im Sinne des Artikels 9 Absatz 2 der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).</p> <p>(2) Zuständige Behörde im Sinne des Artikels 9 Absatz 1 der Richtlinie (EU) 2022/2557 ist im Hinblick auf Aufgaben des Bundes das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Abweichend von Satz 1 ist zuständige Behörde in Bezug auf öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste die Bundesnetzagentur und für alle anderen Betreiber kritischer Anlagen im Sektor Informationstechnik und Telekommunikation das Bundesamt für Sicherheit in der Informationstechnik, in Bezug auf den Sektor Finanz- und Versicherungswesen die Bundesanstalt für Finanzdienstleistungsaufsicht sowie die weiteren Aufsichtsbehörden des Bundes nach Absatz 3 und im Hinblick auf Aufgaben der Länder die zuständigen Landesbehörden nach Absatz 5.</p> <p>(3) Der Bund ist zuständig für den Vollzug dieses Gesetzes in Bezug auf folgende kritische Dienstleistungen:</p> <ol style="list-style-type: none"> 1. Stromversorgung, 2. Gasversorgung, 3. Kraftstoff- und Heizölversorgung, 4. Erzeugung von Wasserstoff gemäß § 54 EnWG, 5. Luftverkehr, soweit er in die Zuständigkeit des Bundesministeriums für Digitales und Verkehr, des Luftfahrtbundesamts und des Bundesamts für Flugsicherung sowie des Bundesministeriums des Innern und für Heimat und der Bundespolizei fällt, 6. Eisenbahnverkehr, soweit er in die Zuständigkeit der bundeseigenen Eisenbahnverkehrsunternehmen und Eisenbahninfrastrukturunternehmen fällt, 7. See- und Binnenschifffahrt mit Ausnahme der Häfen 8. Straßenverkehr in Bezug auf Verkehrssteuerungs- und Leitsysteme sowie intelligente Verkehrssysteme, soweit er in die Zuständigkeit der Autobahn GmbH des Bundes fällt, 9. Wettervorhersage, soweit er in die Zuständigkeit des Deutschen Wetterdienstes fällt, 10. Sprach- und Datenübertragung, 11. Datenspeicherung und -verarbeitung, 12. Bargeldversorgung, 13. kartengestützter Zahlungsverkehr, 14. konventioneller Zahlungsverkehr, 15. Handel mit Wertpapieren und Derivaten sowie die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften, 16. Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende, 17. Betrieb von Bodeninfrastrukturen für den Weltraum, 18. Dienstleistungen, die von Einrichtungen der Bundesverwaltung nach § 5 Absatz 1 erbracht werden. <p>Das Bundesministerium des Innern und für Heimat macht die zuständigen Bundesbehörden im Bundesanzeiger bekannt.</p> <p>(4) Die Länder benennen bis 02. Januar 2025 dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe je eine Landesbehörde als zentralen Ansprechpartner für sektorenübergreifende Angelegenheiten im Zusammenhang mit der Durchführung dieses Gesetzes.</p> <p>(5) Die Länder bestimmen, ob die Landesbehörde nach Absatz 4 oder andere Landesbehörden die Aufgaben nach diesem Gesetz wahrnehmen. Sie teilen dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bis 02. Januar 2026 mit, welche Behörde die Aufgaben nach diesem Gesetz jeweils wahrnimmt.</p> <p>(6) Für Betreiber kritischer Anlagen, für die die Länder zuständig sind, bestimmt sich das zuständige Land nach dem Hauptsitz des Betreibers kritischer Anlagen.</p>	<p>Ungünstig ist, das die Durchsetzung zuerst geregelt wird und danach in §4, wer/was geregelt wird.</p> <p>Hierdurch kann diese Auflistung den Eindruck vermitteln, dass alle hier nicht genannten Branchen nicht dem KRITIS DachG unterliegen. Es sollte, z.B. in einer Anlage, schon jetzt klar gestellt werden, welche Branchen insgesamt dem KRITIS DachG unterstehen und nicht erst in der KRITIS-VO.</p> <p>In dieser Anlage sollte ebenfalls definiert werden, wo die Verantwortlichkeit beim Bund und wo die Verantwortlichkeit bei den Bundesländern liegt.</p> <p>Damit wird sichergestellt, dass die Länder das Gesetz nicht auf weitere Branchen ausweiten, sondern der betroffenen Kreis der Branchen abschließend durch den Bund festgelegt ist.</p> <p>Die Formulierungen sollten konform mit dem NIS2-UmsCG sein. Die Themen, die bereits in der NIS2-UmsCG abschließend für bestimmte Sektoren geregelt wurde, sollten hier nicht mehr im Gesetz geregelt werden.</p> <p>Unternehmen mit Territorialitätsbezug nach NIS2 (Jumelet IT) sollten hier nicht aufgeführt werden.</p> <p>Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.</p>
§4	<p>Anwendungsbereich; kritische Anlagen; Geltungsbereich</p> <p>(1) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 16 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Rechtsverordnung nach § 16 Absatz 1 festgelegten Anlagearten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und diese die durch Rechtsverordnung nach § 16 Absatz 1</p> <p>(2) Über die Identifizierung entsprechend den Vorgaben der Rechtsverordnung nach Absatz 1 in Verbindung mit § 16 Absatz 1 hinaus kann das Bundesministerium des Innern und für Heimat auf Vorschlag der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder der zuständigen Behörde der Länder nach § 3 Absatz 5 sowie im eigenen Betreiben im Rahmen der nach Absatz 1 festgelegten Sektoren und innerhalb der kritischen Dienstleistungen gemäß Rechtsverordnung nach Absatz 1 in Verbindung mit § 16 Absatz 1 weitere Betreiber kritischer Anlagen unter Berücksichtigung der nationalen Risikoanalysen und Risikobewertungen nach § 8 f) sowie den folgenden Kriterien festlegen:</p> <ol style="list-style-type: none"> 1. die Zahl der Nutzer, die die von der betreffenden Anlage erbrachten kritischen Dienstleistung in Anspruch nehmen; 2. das Ausmaß der Abhängigkeit anderer Sektoren oder Branchen von der betreffenden kritischen Dienstleistung; 3. die möglichen Auswirkungen von Ausfällen hinsichtlich Ausmaßes und Dauer auf wirtschaftliche und gesellschaftliche Tätigkeiten, die Umwelt, die öffentliche Ordnung und Sicherheit oder die Gesundheit der Bevölkerung; 4. den Marktanteil des Betreibers der Anlage auf dem Markt für kritische Dienstleistungen oder für die betreffenden kritischen Dienstleistungen; 5. das geografische Gebiet, das von einem Vorfall betroffen sein könnte, einschließlich etwaiger grenzüberschreitender Auswirkungen, unter Berücksichtigung der Schwachstellen, die mit dem Grad der Isolierung bestimmter Arten geografischer Gebiete verbunden sind; 6. die Bedeutung des Betreibers der Anlage für die Aufrechterhaltung der kritischen Dienstleistung in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Erbringung der betreffenden kritischen Dienstleistung. <p>Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe teilt dem Betreiber der betreffenden kritischen Anlage mit, dass er den Verpflichtungen dieses Gesetzes unterliegt und fordert ihn zur Registrierung nach § 6 Absatz 1 auf.</p> <p>(3) Eine kritische Anlage ist ab dem nächsten folgenden durch die Rechtsverordnung nach § 16 Absatz 1 als Stichtag festgelegten Tag keine kritische Anlage mehr, wenn sie die durch die Rechtsverordnung festgelegten Schwellenwerte unterschreitet.</p> <p>(4) Rechtfertigten Tatsachen die Annahme, dass ein Betreiber kritischer Anlagen nach Absatz 2 die dortigen Kriterien nicht mehr erfüllt, stellt dies das Bundesministerium des Innern und für Heimat auf Vorschlag der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder der zuständigen Behörde der Länder nach § 3 Absatz 5 sowie im eigenen Betreiben fest. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe teilt dem Betreiber der betreffenden kritischen Anlage mit, dass er den Verpflichtungen dieses Gesetzes nicht mehr unterliegt.</p> <p>(5) § 3 Absatz 8, § 13 Absatz 2 und § 7 gelten nicht für Betreiber kritischer Anlagen im Sektor Siedlungsabfallentsorgung.</p>	<p>Mindestens Punkt 2. und 3. sind vom Unternehmen nicht beantwortbar, da diese Informationen nicht vorliegen. Kaskadeneffekte sollten, wie auch bei der Einführung des IT-Sicherheitsgesetzes, nicht berücksichtigt werden.</p>

		<p>§ 3 Absatz 8, § 13 Absatz 2 und die §§ 7 bis 12 gelten nicht für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.</p>	<p>Hintergrund ist, dass eine Doppelregulierung vermieden werden soll. Speziell für den Bereich ITK geht das Dachgesetz davon aus, dass durch die TK Gesetzgebung und NIS2 Umsetzung auch ein ausreichender physischer Schutz gefordert wird. Gleiches gilt für, Finanz- und Versicherungswesen. Hier ist DORA einschlägig. Es verbleiben für die betroffenen Unternehmen die folgenden Paragraphen:</p> <p>§6 - Identifizierung als Betreiber einer Kritischen Anlage gem. einer übergreifenden Rechtsverordnung, die noch ausstehend ist, und die damit einhergehende Registrierung als solcher.</p> <p>§14 - Billigungs-, Überwachungs-, und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen. Wobei die Billigungs- und Überwachungspflichten sich auf den §10 beziehen, der ja gem. §4 Absatz 6 nicht gilt. Somit verbleibt nur die Schulungspflicht inkl. Bereitstellung der Nachweise auf Anfrage der Behörden.</p> <p>§19 – Bußgeldvorschriften. Hier ist relevant, dass es ordnungswidrig ist eine kritische Anlage nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zu registrieren und die Dokumente / Auskunft hierzu zu verweigern. Die Höhe der möglichen Geldbuße ist noch offen gehalten.</p> <p>Warum gilt das nicht für die Strom- und Gasversorgung? Hier gibt es auch einen Sicherheitskatalog nach Energiewirtschaftsgesetz bei dem bereits Heute ausführlich physikalischen Sicherheitsthemen behandelt werden.</p> <p>Vorschlag: Wäre es nicht einfacher lediglich die Registrierung nach §6 für diese benannten Branchen zu adressieren.</p>
		<p>(7) Andere bestehende Regelungen, die die Resilienz von Betreibern kritischer Anlagen zum Ziel haben, bleiben von diesem Gesetz unberührt.</p>	<p>Die Identifizierung der "anderen Regelungen" die von diesem Gesetz unberührt bleiben ist für betroffene Unternehmen in der Anwendung und Umsetzung zu komplex. Es sollte ein Gesetz für einen Sektor geben und nicht zwei Gesetze mit zum Teil überscheidenden Anforderungen. Im Zweifel wird zukünftig nicht klar sein, welches Gesetz und welche Behörde die höheren Resilienzanforderungen hat.</p> <p>Bei Verwaltungsentscheidung sollten Maßnahmen zur Steigerung der notwendigen Resilienz bei Betreibern von kritischen Anlagen mit besonderem Gewicht berücksichtigt werden (z.B. Sicherheit vor Denkmalschutz oder Sicherheit vor Transparenzpflichten).</p>
		<p>(8) Risikoanalysen und Risikobewertungen sowie Dokumente und Maßnahmen zur Stärkung der Resilienz, die der Betreiber einer kritischen Anlage auf Grund anderer öffentlich-rechtlicher Verpflichtungen ergriffen hat, gelten als Analysen, Bewertungen, Dokumente und Maßnahmen nach §§ 9 bis 11, soweit sie diesen gleichwertig sind. Die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 stellen die Gleichwertigkeit im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik fest, die zuständigen Behörden der Länder nach § 3 Absatz 5 stellen die Gleichwertigkeit im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik fest. Die tatsächlichen Feststellungen anderer Behörden zu Risikoanalysen und Risikobewertungen sowie Dokumenten und Maßnahmen zur Stärkung der Resilienz nach Satz 1 sind zugunsten des Betreibers der kritischen Anlage bindend</p>	<p>Hier sollte grundsätzlich die Eignung von der Behörde festgelegt werden z.B. Risikoanalysen und Maßnahmen, die auf Basis eines internationalen oder nationalen (B35) Standards erstellt wurden, sollen durch das BBK auch für das KRITIS Dachgesetz als geeignet anerkannt werden. Eine Einzelprüfung pro Betreiber ist unrealistisch.</p>
95		<p>Einrichtungen der Bundesverwaltung</p>	
	(1)	(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind die Bundesministerien und das Bundeskanzleramt	
	(2)	(2) Einrichtungen der Bundesverwaltung, die Tätigkeiten ausüben in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, sind von den Verpflichtungen nach diesem Gesetz ausgenommen. Das Ausnahmeverfahren bestimmt sich nach § 17.	
	(3)	(3) Für Einrichtungen der Bundesverwaltung, die nicht zugleich Betreiber kritischer Anlagen nach § 4 sind, sind die Pflichten für Betreiber kritischer Anlagen nach §§ 6, 9, § 10 Absatz 1 bis 5, 7 bis 10, §§ 11 bis 13, 17 und 18 entsprechend anzuwenden, soweit keine abweichenden Regelungen festgelegt werden.	Öffentliche Sicherheit ist für den Betrieb Kritischer Anlagen essentiell und darf nicht von diesen Regelungen ausgenommen werden.
	(4)	(4) §§ 7 und 14 sind nicht auf Einrichtungen der Bundesverwaltung anzuwenden.	
	(5)	(5) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe legt für Einrichtungen nach Absatz 1 zur Konkretisierung der Resilienzmaßnahmen nach § 10 Absatz 1 Mindeststandards im Einvernehmen mit den Bundesressorts und im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik fest.	
	(6)	(6) § 11 Absatz 6 gilt mit der Maßgabe, dass Maßnahmen zur Mängelbeseitigung durch die zuständige Behörde des Bundes nach § 3 Absatz 3 nur im Einvernehmen mit der jeweiligen Einrichtung der Bundesverwaltung anzuordnen sind.	
96		<p>Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt</p>	
	(1)	<p>(1) Ein Betreiber einer kritischen Anlage ist verpflichtet, spätestens drei Monate nach dem erstmaligen oder erneuten als Betreiber kritischer Anlagen gilt, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe über eine gemeinsam vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik eingerichtete Registrierungsmöglichkeit folgende Angaben zu übermitteln:</p> <p>1. den Namen des Betreibers der kritischen Anlage, einschließlich der Rechtsform und soweit einschlägig der Handelsregisternummer,</p> <p>2. die Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adresse, öffentliche IP-Adressbereiche und Telefonnummern, sowie falls einschlägig die Anschrift des Hauptsitzes,</p> <p>3. den relevanten Sektor und soweit einschlägig die Branche und kritische Dienstleistung,</p> <p>4. die für die von ihm ermittelten Anlagen die Anlagenkategorie und Versorgungskennzahlen gemäß der Rechtsverordnung nach § 16 Absatz 1 sowie den Standort der Anlagen und deren Versorgungsgebiet,</p> <p>5. eine Auflistung der Mitgliedstaaten der Europäischen Union, in denen der Betreiber der kritischen Anlage wesentliche Dienste im Sinne der Richtlinie (EU) 2022/2557 und der Delegierten Verordnung (EU) 2023/2450 erbringt,</p> <p>6. eine Kontaktstelle, über die der Betreiber der kritischen Anlage jederzeit erreichbar ist.</p>	<p>Inwieweit werden bestehende Registrierungen als KRITIS Betreiber nach NIS2/UmucG übernommen? Registrierung für NIS2 bis zum 17.01.2025?</p> <p>Manche Angaben sind nicht konstant (z.B. IP Adressen, Telefonnummern), in welcher Form Rhythmus müssen sie aktualisiert werden?</p>
	(2)	(2) Rechtfertigten Tatsachen die Annahme, dass ein Betreiber kritischer Anlagen seine Pflicht zur Registrierung nicht erfüllt, so hat dieser dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe auf Verlangen die aus Sicht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen. Sollten Geheimheitsinteressen oder überwiegende Sicherheitsinteressen dem entgegenstehen, ist dies nachvollziehbar darzulegen und zu begründen.	
	(3)	(3) Wenn der Betreiber kritischer Anlagen seine Pflicht zur Registrierung nicht erfüllt, kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach Anhörung des betroffenen Betreibers die Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder im Einvernehmen mit der zuständigen Behörde der Länder nach § 3 Absatz 5 selbst vornehmen. Das Bundesamt für Sicherheit in der Informationstechnik und die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 oder die zuständigen Behörden der Länder nach § 3 Absatz 5 können dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Vorschläge für die Registrierung weiterer Betreiber kritischer Anlagen unterbreiten und übermitteln dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die erforderlichen Informationen zur Identifizierung der Betreiber kritischer Anlagen.	
	(4)	(4) Für die nach § 4 Absatz 2 identifizierten Betreiber kritischer Anlagen gilt Absatz 3 entsprechend.	
	(5)	(5) Dem Betreiber kritischer Anlagen wird die für ihn jeweils federführend zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe spätestens zwei Wochen nach der Registrierung mitgeteilt.	
	(6)	(6) Die Verpflichtungen nach § 9 greifen erstmals neun Monate, die Verpflichtungen nach § 10 bis § 12 erstmals zehn Monate nach der Registrierung des Betreibers kritischer Anlagen.	Wenn ein Unternehmen 9 Monate für die Erstellung des Resilienzplanes benötigt, bleibt noch 1 Monat für die Implementierung der Maßnahmen. Bauliche Maßnahmen sind so nicht umzusetzen (alleine Baugenehmigungen sind so schnell nicht herbei zu führen). Siehe auch angehangen Zeitstrahl
	(7)	(7) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.	Ziel sollte eine gemeinsame Plattform zur Registrierung sein.
97		<p>Kritische Einrichtungen von besonderer Bedeutung für Europa</p>	Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.
	(1)	(1) Ein Betreiber kritischer Anlagen nach § 4 Absatz 1 gilt als kritische Einrichtung von besonderer Bedeutung für Europa, wenn	
		<p>1. er für oder in mindestens sechs oder mehr Mitgliedstaaten der Europäischen Union den gleichen oder ähnlichen wesentlichen Dienst erbringt und</p> <p>2. ihm von der Europäischen Kommission über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mitgeteilt wurde, dass er als kritische Einrichtung von besonderer Bedeutung für Europa gilt.</p>	
	(2)	(2) Der Betreiber kritischer Anlagen teilt dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Falle des Absatzes 1 Nummer 1 mit, welche wesentlichen Dienste er für welche oder in welchen Mitgliedstaaten anbietet. Das Bundesministerium des Innern und für Heimat teilt diese Informationen der Europäischen Kommission unverzüglich mit.	
	(3)	(3) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe leitet die Mitteilung der Europäischen Kommission, einen Betreiber kritischer Anlagen als kritische Einrichtung von besonderer Bedeutung für Europa zu betrachten, unverzüglich an diesen weiter.	
	(4)	(4) Das Bundesministerium des Innern und für Heimat kann einen Antrag bei der Europäischen Kommission auf Einrichtung einer Beratungsmission zur Bewertung der Maßnahmen stellen, die eine kritische Einrichtung mit besonderer Bedeutung für Europa ergriffen hat, um ihre Verpflichtungen nach §§ 8 bis 11 zu erfüllen.	Was genau ist eine "Beratungsmission"? Legt diese verbindlich zu erfüllende Maßnahmen fest, die durch den Betreiber der kritischen Anlage umzusetzen ist? Der Begriff sollte in §2 definiert werden.
	(5)	(5) Auf Antrag der Europäischen Kommission oder eines Mitgliedstaats, für den oder in dem eine kritische Dienstleistung erbracht wird, übermittelt das Bundesministerium des Innern und für Heimat der Europäischen Kommission,	
		<p>1. Teile der Risikoanalysen und Risikobewertungen der kritischen Einrichtung mit besonderer Bedeutung für Europa nach § 9,</p> <p>2. eine Auflistung der Maßnahmen der kritischen Einrichtung mit besonderer Bedeutung für Europa nach § 10 und</p> <p>3. eine Auflistung der Aufsichts- und Durchsetzungsmaßnahmen, die die für die kritische Einrichtung zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 gegenüber der kritischen Einrichtung mit besonderer Bedeutung für Europa ergriffen hat.</p>	

	(6)	(6)Die kritischen Einrichtungen mit besonderer Bedeutung für Europa unterstützen das Bundesministerium des Innern und für Heimat bei der Zurverfügungstellung der Informationen für die Beratungsmission. Die kritischen Einrichtungen von besonderer Bedeutung für Europa gewähren der Beratungsmission nach Absatz 4 Zugang zu Informationen, Systemen und Anlagen im Zusammenhang mit der Erbringung ihrer kritischen Dienstleistung, die zur Durchführung der betreffenden Beratungsmission erforderlich sind. Sie beziehen die Stellungnahme der Europäischen Kommission auf Grundlage des Berichts der Beratungsmission bei der fortlaufenden Umsetzung der Maßnahmen nach §§ 9, 10 und 12 mit ein.	
	(7)	(7)Für den Fall, dass die Europäische Kommission einen oder mehrere Durchführungsrechtsakte gemäß Artikel 18 Absatz 6 der Richtlinie (EU) 2022/2557 erlässt, in der das Verfahren im Zusammenhang mit der Beratungsmission konkretisiert wird, geht dieser oder gehen diese den Vorschriften des Absatzes 4 bis 6 vor.	
88	Nationale Risikoanalysen und Risikobewertungen		Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.
	(1)	(1)Die für die jeweiligen kritischen Dienstleistungen nach § 3 Absatz 3 und 5 zuständigen Bundesministerien und Landesministerien führen alle vier Jahre oder auf Veranlassung und erstmalig bis 17. Januar 2026 für die auf der Grundlage der Rechtsverordnung nach § 16 Absatz 1 bestimmten kritischen Dienstleistungen nationale Risikoanalysen und Risikobewertungen durch, die mindestens Folgendes berücksichtigen: 1.naturbedingte, klimatische und vom Menschen verursachte Risiken, die die Handlungsfähigkeit der Wirtschaft bedrohen, darunter a)sektorübergreifende und grenzüberschreitende Risiken, b)Unfälle, Naturkatastrophen und gesundheitliche Notlagen sowie c)hybride Bedrohungen, sicherheitsgefährdende oder geheimdienstliche Tätigkeiten einer fremden Macht oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31.03.2017, S. 6), 2.alle wesentlichen Risiken für den Binnenmarkt und die Bevölkerung, die sich aus dem Ausmaß der Abhängigkeit zwischen den in § 4 Absatz 1 genannten Sektoren ergeben und die die Wirtschaftsstabilität beeinträchtigen, einschließlich a)dem Ausmaß der Abhängigkeit von in anderen Mitgliedstaaten und Drittstaaten ansässigen kritischen Einrichtungen sowie b)den Auswirkungen, die eine in einem Sektor auftretende erhebliche Störung auf andere Sektoren haben kann, 3.die allgemeine Risikobewertung nach Artikel 6 Absatz 1 des Beschlusses Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924), 4.die sonstige Risikobewertungen, die im Einklang mit den Anforderungen der entsprechenden sektorspezifischen Rechtsakte der Union sind, einschließlich a)der Verordnung (EU) 2017/1938 des Europäischen Parlaments und des Rates vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung und zur Aufhebung der Verordnung (EU) Nr. 994/2010 (ABl. L 280 vom 28.10.2017, S. 1), b)der Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorwarnung im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG (ABl. L 158 vom 14.06.2019, S. 1), c)der Richtlinie 2007/60/EG des Europäischen Parlaments und des Rates vom 23. Oktober 2007 über die Bewertung und das Management von Hochwasserrisiken (ABl. L 288 vom 06.11.2007, S. 27), d)der Richtlinie 2012/18/EU des Europäischen Parlaments und des Rates vom 4. Juli 2012 zur Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen, zur Änderung und anschließenden Aufhebung der Richtlinie 96/82/EG des Rates (ABl. L 197 vom 24.07.2012, S. 1), (2)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann die methodischen und inhaltlichen Vorgaben für die nationalen Risikoanalysen und Risikobewertungen nach Absatz 1 festlegen. Die Festlegung nach Satz 1 erfolgt durch Verwaltungsvorschrift. (3)(3)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe wertet die nach Absatz 1 durch die Bundesministerien und Landesministerien durchgeführten nationalen Risikoanalysen und Risikobewertungen sektorenübergreifend aus. (4)(4)Für die Zwecke des Absatz 1 Nr. 2 sowie des Absatz 3 arbeiten die Bundesministerien und Landesministerien nach Absatz 1 sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mit den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit den zuständigen Behörden aus Drittstaaten zusammen. (5)(5)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe stellt den Betreibern kritischer Anlagen, den für die nationalen Risikobewertungen jeweils zuständigen Bundesministerien und Landesministerien sowie den zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und den zuständigen Behörden der Länder nach § 3 Absatz 5 die für sie wesentlichen Elemente der Risikoanalysen und Risikobewertungen zur Verfügung.	Die Wirtschaft sollte zwingend in §8 mit berücksichtigt werden... z.B. Beratung durch Branchenvende Hoheitlicher Schutz muss bei den nationalen Risikoanalysen berücksichtigt werden. Gegen manche Bedrohungen kann ein Betreiber sich nicht (alleine) schützen. Kaskaden Effekte: Diese wurden bei dem IT-SIG explizit nicht betrachtet, da ansonsten keine Risikoanalysen mit Auswahl von geeigneten wirtschaftlich vertretbaren Resilienzmaßnahmen möglich sind (Bsp. Stromversorgung... lokaler Stromausfall führt zu einem Blackout in Europa, mit allem was an Industrie- und Privatkunden dahinter hängt).
89	Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen		Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.
	(1)	(1)Betreiber kritischer Anlagen führen auf Grundlage der nationalen Risikoanalysen und Risikobewertungen nach § 8 und anderer vertrauenswürdiger Informationsquellen mindestens alle vier Jahre Risikoanalysen und Risikobewertungen durch, die Folgendes berücksichtigen: 1.die in § 8 Absatz 1 Nr. 1 genannten Risiken, 2.Risiken, die die Handlungsfähigkeit der Wirtschaft beeinträchtigen und die sich aus Folgendem ergeben: a)dem Ausmaß der Abhängigkeit des Betreibers kritischer Anlagen von den kritischen Dienstleistungen, die von anderen Betreibern kritischer Anlagen in anderen Sektoren auch in benachbarten Mitgliedstaaten und Drittstaaten erbracht werden und b)dem Ausmaß der Abhängigkeiten anderer Sektoren von der kritischen Dienstleistung, die von einem Betreiber kritischer Anlagen auch in benachbarten Mitgliedstaaten und Drittstaaten erbracht wird.	Kaskaden Effekte: Diese wurden bei dem IT-SIG explizit nicht betrachtet, da ansonsten keine Risikoanalysen mit Auswahl von geeigneten wirtschaftlich vertretbaren Resilienzmaßnahmen möglich sind (Bsp. Stromversorgung... lokaler Stromausfall führt zu einem Blackout in Europa, mit allem was an Industrie- und Privatkunden dahinter hängt)... da müsste sich ja jeder vor einem langfristigen europaweiten Stromausfall, der durch einen lokalen Problem in Rumänien verursacht wurde schützen? Das geht noch weniger als andersrum! Bezüglich der wesentlichen Elemente der Risikoanalysen und Risikobewertungen, welche durch das BBK den Betreibern kritischer Anlagen zur Verfügung gestellt werden, stellt sich die Frage, ob und wie diese nach der Verschlusssachenanweisung (VSA) eingestuft werden. Nicht alle Organisationen unterliegen der Geheimschutzbetreuung. Wie wird sichergestellt, dass diese Organisationen die erforderlichen Informationen dennoch erhalten können? Bei einer VS-Einstufung kämen auf diese Organisationen erhebliche zusätzliche organisatorische und technische Mehraufwände zu.
	(2)	(2)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann inhaltliche und methodische Vorgaben einschließlich Vorlagen und Muster für die Risikoanalysen und Risikobewertungen nach Absatz 1 festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.	Es können sich teilweise Probleme ergeben, wenn, wie im Entwurf formuliert, inhaltliche und methodische Vorgaben für die Risikoanalysen und -bewertungen festgelegt werden. Beispielsweise, wenn bereits etablierte Risikomanagementstandards bestehen und durch das BBK konträre Vorgaben/Vorlagen festgelegt werden. Es ist zwingend, dass die Methodiken für kleinere Betreiber auch umsetzbar sein müssen, ohne das hierzu völlig überzogene Kosten aufgrund der Beauftragung von teuren Spezialisten entstehen. Die Wirtschaftlichkeit wird an dieser Stelle nicht mehr betrachtet, sondern für alle eine allgemeine Festlegung getroffen. Unverbindliche Vorlagen oder Muster könnten insbesondere neu betroffenen Betreibern helfen. Inhaltliche und methodische Vorgaben sollten auf keinen Fall gemacht werden. Die bisherige Gesetzgebung BSI-G und die bisherigen Gesetze überlassen den Betreibern die Wahl der Methodik und die Durchführung (siehe z.B. LKSG, KRITIS-VO). Dies sollte auch zukünftig so bleiben. Eine aktive Kommunikation über die Veröffentlichung von solchen Mustern bzw. Vorlagen ist wünschenswert.
910	Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan		Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.
	(1)	(1)Betreiber kritischer Anlagen sind nach Ablauf von 10 Monaten nach Registrierung verpflichtet, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen, die erforderlich sind, um 1.das Auftreten von Vorfällen zu verhindern, 2.einen angemessenen physischen Schutz ihrer Liegenschaften und kritischen Anlagen zu gewährleisten, 3.auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen, 4.nach Vorfällen die Wiederherstellung der kritischen Dienstleistung zu gewährleisten, 5.ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, einschließlich des Personals externer Dienstleister, und 6.das Personal für die unter den Nummern 1 bis 5 genannten Maßnahmen durch Informationsmaterialien, Schulungen und Übungen zu sensibilisieren. Die Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Vorfalls zum Risiko eines Vorfalls angemessen erscheint.	Wichtiger Satz: "Die Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Vorfalls zum Risiko eines Vorfalls angemessen erscheint." in der Begründung wurde ergänzt: "Dabei können auch wirtschaftliche Aspekte berücksichtigt werden." ... warum nicht auch im Gesetzestext selber verankern. Frist von 10 Monaten ist unrealistisch (Siehe auch "Timeline")
	(2)	(2)Die Maßnahmen nach Absatz 1 sind auf Grundlage der nationalen Risikoanalysen und Risikobewertungen nach § 8 sowie der Risikoanalyse und Risikobewertung des Betreibers der kritischen Anlage nach § 9 zu treffen. Der Stand der Technik soll eingehalten werden.	
	(3)	(3)Zu den Maßnahmen nach Absatz 1 können die folgenden zählen: 1.zum Zweck des Absatzes 1 Satz 1 Nummer 1: a)Maßnahmen der Notfallvorsorge und b)Maßnahmen zur Anpassung an den Klimawandel, 2.zum Zweck des Absatzes 1 Satz 1 Nummer 2: a)Maßnahmen des Objektschutzes, darunter das Aufstellen von Zäunen und Sperren, b)Instrumente und Verfahren für die Überwachung der Umgebung, c)der Einsatz von Detektionsgeräten und d)Zugangskontrollen, 3.zum Zweck des Absatzes 1 Satz 1 Nummer 3: a)Risiko- und Krisenmanagementverfahren und -protokolle und b)vorgegebene Abläufe im Alarmfall, 4.zum Zweck des Absatzes 1 Satz 1 Nummer 4: a)Maßnahmen zur Aufrechterhaltung des Betriebs, darunter die Notstromversorgung und b)die Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen, 5.zum Zweck des Absatzes 1 Satz 1 Nummer 5: a)die Festlegung aa)von Kategorien von Personal, das kritische Funktionen wahrnimmt, bb)von Zugangsrechten zu Liegenschaften, kritischen Anlagen und zu sensiblen Informationen sowie cc)von angemessenen Schulungsanforderungen und Qualifikationen und d)unbeschadet der Vorschriften über Zuverlässigkeitsüberprüfungen die Berücksichtigung von Verfahren für Zuverlässigkeitsüberprüfungen und die Benennung von Kategorien von Personal, die Zuverlässigkeitsüberprüfungen durchlaufen müssen, und 6.zum Zweck des Absatzes 1 Satz 1 Nummer 6: a)Schulungen, b)die Bereitstellung von Informationsmaterial und c)Übungen.	Dem UP KRITIS scheint dieser § ausreichend als Grundlage für die zukünftigen branchenspezifischen Resilienzstandards und braucht nicht weiter ergänzt werden.

	(4)	(4)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe erstellt zur Konkretisierung von Absatz 1 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von sektorenübergreifenden Mindestanforderungen und veröffentlicht diesen auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe. Die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die zuständigen Behörden der Länder nach § 3 Absatz 5 sind bei der Erarbeitung des Katalogs von sektorenübergreifenden Mindestanforderungen durch Anhörung zu beteiligen. Die betroffenen Betreiber kritischer Anlagen und die betroffenen Wirtschaftsverbände sind anzuhören.	Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben
	(5)	(5)Die für die kritischen Dienstleistungen jeweils zuständigen Bundesministerien können Rechtsverordnungen gemäß § 16 Absatz 2 zur sektorspezifischen Konkretisierung von Resilienzmaßnahmen erlassen.	Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben
	(6)	(6)Betreiber kritischer Anlagen und ihre Branchenverbände können branchenspezifische Resilienzstandards zur Erfüllung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und 1.im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder 2.im Einvernehmen mit der zuständigen Behörde der Länder nach § 3 Absatz 5.	Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben
	(7)	Abweichend von Absatz 6 legt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe für Einrichtungen der Bundesverwaltung nach § 5 Absatz 1 zur Konkretisierung der Resilienzmaßnahmen nach Absatz 1 Mindeststandards im Einvernehmen mit den fachlich zuständigen Bundesressorts und im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik fest.	
	(8)	(8)Für den Fall, dass die Europäische Kommission einen oder mehrere Durchführungsrechtsakte gemäß Artikel 13 Absatz 6 der Richtlinie (EU) 2022/2557 erlässt, in der die technischen und methodischen Spezifikationen für die Maßnahmen nach Absatz 1 konkretisiert werden, geht dieser oder gehen diese den Vorschriften nach den Absätzen 1 bis 7 vor.	
	(9)	(9)Betreiber kritischer Anlagen müssen die Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen und diesen anwenden. Aus dem Resilienzplan müssen die den Maßnahmen zugrunde liegenden Erwägungen einschließlich der Risikoanalysen und Risikobewertungen nach § 9 hervorgehen.	Den Wirtschaftsvertretern des UP KRITIS ist nicht klar, was mit einem „Resilienzplan“ adressiert ist. Sind damit a) Maßnahmen die bereits implementiert sind, oder b) ergänzende und neue Maßnahmen die zukünftig implementiert werden sollen, da noch Maßnahmen fehlen, oder c) Beides (a) und b)) adressiert. Auch ist unklar, in welcher Detailtiefe hier gemeldet werden muss. Hier nochmal der Hinweis, dass diese Informationen, je nach Detailtiefe, äußerst sensible Informationen sind.
	(10)	(10)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann den Betreibern kritischer Anlagen Vorlagen und Muster für einen Resilienzplan nach Absatz 9 zur Verfügung stellen. Vorlagen und Muster werden auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe veröffentlicht.	
§11	Nachweise; behördliche Anordnungen		
	(1)	(1)Zum Zwecke der Überprüfung der Einhaltung der Maßnahmen nach § 10 Absatz 1 kann die für den Betreiber kritischer Anlagen zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe vom Bundesamt für Sicherheit in der Informationstechnik die Übersendung derjenige(n) Bestandteile des Nachweises der Einhaltung der Maßnahmen nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen] verlangen, die für die Überprüfung der Einhaltung der Maßnahmen nach § 10 Absatz 1 erforderlich sind. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe erstellt hierzu im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik eine sektorenübergreifende Liste der für physische Resilienzmaßnahmen relevanten Bestandteile des Nachweises nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen]].	Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation. Der UP KRITIS empfiehlt, wie im NIS2UmUG, die Nachweiserbringung frühestens 2 Jahre nach Beginn der Umsetzung/Implementierung der physischen Sicherheitsmaßnahmen zu starten. Somit können sowohl bereits implementierte Maßnahmen als auch zukünftig geplante Maßnahmen auf deren Eignung geprüft werden.
	(2)	(2)Sofern die übermittelten Informationen zur Feststellung der Erfüllung der Verpflichtungen nach § 10 Absatz 1 nicht ausreichen, kann die für den Betreiber kritischer Anlagen zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 den Betreiber kritischer Anlagen zur Vorlage weiterer Informationen und geeigneter Nachweise zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 auffordern. Sie kann die Vorlage des Resilienzplans sowie eines geeigneten Nachweises zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 verlangen.	Der UP KRITIS empfiehlt, wie im NIS2UmUG, die Nachweiserbringung frühestens 2 Jahre nach Beginn der Umsetzung/Implementierung der physischen Sicherheitsmaßnahmen zu starten. Somit können sowohl bereits implementierte Maßnahmen als auch zukünftig geplante Maßnahmen auf deren Eignung geprüft werden.
	(3)	(3)Der Nachweis kann durch Audits erfolgen. Der Betreiber kritischer Anlagen übermittelt der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder der zuständigen Behörde der Länder nach § 3 Absatz 5 auf Anforderung die Ergebnisse der durchgeführten Audits einschließlich der dabei aufgedeckten Mängel. Die zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 kann die Vorlage der Dokumentation, die der Überprüfung durch einen Audit oder auf andere Weise zugrunde gelegt wurde, verlangen.	
	(4)	(4)Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe legt zur Ausgestaltung des Verfahrens der Erbringung des Nachweises und der Audits nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber kritischer Anlagen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik fest. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.	
	(5)	(5)Bei erheblichen Zweifeln an der Einhaltung der Verpflichtungen nach § 10 Absatz 1 kann die zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 die Einhaltung der Verpflichtungen nach § 10 Absatz 1 überprüfen. Bei der Durchführung der Überprüfung kann es sich um einen qualifizierten unabhängigen Dritten handeln. Der Betreiber kritischer Anlagen hat der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder der zuständigen Behörde der Länder nach § 3 Absatz 5 und den in deren Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung kann die zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 Gebühren und Auslagen bei dem Betreiber kritischer Anlagen erheben.	
	(6)	(6)Die zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 kann bei Mängeln die Vorlage eines geeigneten Mängelbeseitigungsplans und Maßnahmen zur Beseitigung der Mängel innerhalb einer angemessenen Frist anordnen, sofern diese angeordneten Maßnahmen nicht im Widerspruch zu Anforderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen] stehen. Sie kann die Vorlage eines geeigneten Nachweises der Mängelbeseitigung verlangen. Absatz 3 gilt entsprechend.	
§12	Meldewesen für Vorfälle		
			Nach §4 Abs6 nicht relevant für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informations-technik und Telekommunikation.

	(1)	(1) Betreiber kritischer Anlagen sind verpflichtet, Vorfälle, die die Erbringung kritischer Dienstleistungen erheblich stören oder erheblich stören könnten, unverzüglich an eine vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik eingerichtete gemeinsame Meldestelle zu melden.	Es sollte weiterhin der Grundsatz „Ein Vorfall - Eine Meldung“ gelten. Daneben ist anzumerken, dass ein Informationsfluss vom BBK an die Betreiber der kritischen Anlagen weiterhin nicht angedacht ist. Neben den Meldungen im dem zentralen Meldeportal an das BBK/BSI, welche bei Bedarf an die BNetzA (auch für Meldeprozesse, die es diesbezüglich in Richtung Versorgungssicherheit schon gibt, z.B. EnWG §52), dem BKA oder dem Verfassungsschutz weitergegeben werden, wäre es wünschenswert auch weitere behördliche Meldeprozesse bei Sicherheitsvorfällen hierüber zu unterstützen (z.B. Datenschutzbehörden, sonstige Aufsichtsbehörden). Im Finanzsektor ist dieses durch DORA bereits umgesetzt.
	(2)	(2) Die Meldungen müssen die verfügbaren Informationen enthalten, die erforderlich sind, damit Art, Ursache und mögliche, auch grenzüberschreitende, Auswirkungen und Folgen des Vorfalls nachvollzogen und ermittelt werden können. Insbesondere sind folgende Angaben zu machen: 1. die Anzahl und Anteil der von der Störung Betroffenen, 2. die bisherige und voraussichtliche Dauer der Störung sowie 3. das betroffene geografische Gebiet der Störung, unter Berücksichtigung des Umstands, ob das Gebiet geografisch isoliert ist.	
	(3)	(3) Betreiber kritischer Anlagen übermitteln eine erste Meldung bis spätestens 24 Stunden nach Kenntnis des Vorfalls. Soweit dies zu diesem Zeitpunkt möglich ist, enthält die Meldung die Angaben nach Absatz 2. Spätestens einen Monat nach Kenntnis des Vorfalls ist ein ausführlicher Bericht zu übermitteln.	
	(4)	(4) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber kritischer Anlagen und der betroffenen Wirtschaftsverbände und im Benehmen mit dem Bundesamt für Sicherheit der Informationstechnik festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.	
	(5)	(5) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe unterrichtet die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten, sofern der Vorfall erhebliche Auswirkungen auf Betreiber kritischer Anlagen und die Aufrechterhaltung der Erbringung wesentlicher Dienste im Sinne der Richtlinie (EU) 2022/2557 in mindestens einem Mitgliedstaat haben könnte.	
	(6)	(6) Hat ein Vorfall erhebliche Auswirkungen auf die Kontinuität der Erbringung wesentlicher Dienste im Sinne der Richtlinie (EU) 2022/2557 für oder in mindestens sechs Mitgliedstaaten oder könnte er solche Auswirkungen haben, so meldet das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe diesen Vorfall der Europäischen Kommission.	
	(7)	(7) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann dem von dem Vorfall betroffenen Betreiber kritischer Anlagen sachdienliche Folgeinformationen übermitteln.	
	(8)	(8) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe übermittelt den zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und den zuständigen Behörden der Länder nach § 3 Absatz 5 sowie den für die nationalen Risikobewertungen zuständigen Bundesministerien und Landesministerien nach § 8 Absatz 1 Auswertungen zu Meldungen von Vorfällen.	
	(9)	(9) Liegt die Offenlegung des Vorfalls im öffentlichen Interesse, so kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach Anhörung des Betreibers der betreffenden kritischen Anlage die Öffentlichkeit über den Vorfall informieren oder den Betreiber einer kritischen Anlage verpflichten, dies zu tun.	
§13		Unterstützung der Betreiber kritischer Anlagen	
	(1)	Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe stellt Betreibern kritischer Anlagen Vorlagen, Muster und Leitlinien zur Umsetzung der Verpflichtungen nach diesem Gesetz zur Verfügung. Es kann zu diesem Zweck auch Beratungen, Schulungen und Übungen anbieten.	Der Anregung, die in der CER-Richtlinie enthaltenen Unterstützungsmaßnahmen (u.a. beschleunigtes ZUP-Verfahren (Zuverlässigkeitsüberprüfung), Vergabe staatlicher Beihilfen) in das KRITIS-DachG aufzunehmen, wurde nicht entsprochen. Enorme Aufwände für die Wirtschaft, die in der CER §4 2e angedachten Unterstützungen wären in der nationalen KRITIS Resiliensstrategie zu berücksichtigen.
	(2)	(2) Das Bundesministerium des Innern und für Heimat kann bei der Europäischen Kommission einen Antrag auf Organisation einer Beratungsmission zur Bewertung der Maßnahmen stellen, die ein Betreiber kritischer Anlagen ergriffen hat, um seine Verpflichtungen nach §§ 9 bis 12 zu erfüllen.	Das gesamte Themenfeld "Beratungsmission" ist dem UP KRITIS unklar.
§14		Billigungs-, Überwachungs-, und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen	Der Geschäftsleiter ist nicht einheitlich definiert. Die Begriffe Geschäftsführung oder -leitung wäre eindeutig .
	(1)	(1) Geschäftsleiter von Betreibern kritischer Anlagen sind verpflichtet, die von diesen Betreibern kritischer Anlagen zur Einhaltung von § 10 ergriffenen Maßnahmen zu billigen und ihre Umsetzung zu überwachen. Ein Verzicht des Betreibers kritischer Anlagen auf Ersatzansprüche aufgrund einer Verletzung der Pflichten nach Absatz 1 oder ein Vergleich des Betreibers kritischer Anlagen über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.	Der vorliegende Entwurf entspricht nun mehr den sehr hohen Haftungsregelungen sowie Schulungs- und Überwachungspflichten für Geschäftsleiter aus NIS2. Für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation gelten nach § 4 Abs. 6 verschiedene Ausnahmen, insbesondere der §§ 7 bis 12. Daher entfällt u.E. auch die Billigungs- und Überwachungspflicht des Absatz 1. Da somit für diese Branchen der §10 nicht anwendbar und es ist unklar, was dann in diesen Fällen für diese Branchen gemeint ist.
	(2)	(2) Die Geschäftsleiter von Betreibern kritischer Anlagen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken und deren Auswirkungen auf die von dem Betreiber der kritischen Anlage eingebrachten Dienstleistungen zu erwerben. Der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder der zuständigen Behörden der Länder nach § 3 Absatz 5 ist ein Nachweis hierüber auf Nachfrage vorzulegen.	Für Betreiber kritischer Anlagen in den Sektoren Bankwesen, Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation gelten nach § 4 Abs. 6 verschiedene Ausnahmen, insbesondere der §§ 7 bis 12. Daher entfällt u.E. auch die Billigungs- und Überwachungspflicht des Absatz 1. Vor diesem Hintergrund erscheint auch eine Schulungspflicht für Geschäftsleiter entbehrlich.
§15		Berichtspflichten	
	(1)	(1) Das Bundesministerium des Innern und für Heimat übermittelt folgende Informationen an die Europäische Kommission: 1. innerhalb von drei Monaten nach Durchführung einer nationalen Risikoanalyse und Risikobewertung jeweils aufgeschlüsselt nach den im Anhang der Richtlinie (EU) 2022/2557 genannten Sektoren und Teilssektoren Informationen a) über die ermittelten Arten von Risiken und b) die Ergebnisse dieser Risikoanalysen und Risikobewertungen, 2. nach der Ermittlung der Betreiber kritischer Anlagen unverzüglich und anschließend alle vier Jahre a) eine Liste der wesentlichen Dienste nach Artikel 7 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2557, b) die Zahl der Betreiber kritischer Anlagen für jeden im Anhang der Richtlinie (EU) 2022/2557 genannten Sektor und Teilssektor und für jeden wesentlichen Dienst im Sinne der Richtlinie (EU) 2022/2557 sowie c) die Schwellenwerte, die in der Rechtsverordnung nach § 16 Absatz 1 zur Spezifizierung eines oder mehrerer der in Artikel 7 Absatz 1 der Richtlinie (EU) 2022/2557 genannten Kriterien festgelegt werden.	
	(2)	(2) Das Bundesministerium des Innern und für Heimat übermittelt der Europäischen Kommission und der Gruppe für die Resilienz kritischer Einrichtungen zur Unterrichtung anderer Mitgliedstaaten bis zum 17. Juli 2028 und danach alle zwei Jahre einen zusammenfassenden Bericht über die Anzahl und die Art 1. der eingegangenen Meldungen nach § 12 und 2. der auf Grundlage von § 12 Absatz 5 ergriffenen Maßnahmen.	
	(3)	(3) Informationen, deren Offenlegung wesentlichen nationalen Interessen im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung entgegenlaufen würden, sind von der Übermittlung von Informationen nach Absatz 1 und Absatz 2 ausgeschlossen.	
	(4)	(4) Für die Zwecke von Absatz 1 Nr. 1 a und b übermitteln die für die jeweiligen kritischen Dienstleistungen nach § 3 Absatz 3 und 5 zuständigen Bundesministerien und Landesministerien die erforderlichen Informationen an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Das Nähere regelt eine Verwaltungsvorschrift.	
	(5)	(5) Für die Zwecke von § 7 Absatz 5 übermitteln die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 oder die zuständigen Behörden der Länder nach § 3 Absatz 5 dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Teile der Risikoanalysen und Risikobewertungen der kritischen Einrichtung mit besonderer Bedeutung für Europa, eine Auflistung der Maßnahmen der kritischen Einrichtung mit besonderer Bedeutung für Europa nach § 10 Absatz 1 und eine Auflistung der Aufsichts- und Durchsetzungsmaßnahmen, die die für die kritische Einrichtung mit besonderer Bedeutung für Europa zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 gegenüber der kritischen Einrichtung mit besonderer Bedeutung für Europa nach § 11 ergriffen hat. Das Nähere regelt eine Verwaltungsvorschrift.	
	(6)	(6) Die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die zuständigen Behörden der Länder nach § 3 Absatz 5 übermitteln dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe jährlich einen zusammenfassenden Bericht über die Aufsichtsmaßnahmen nach § 11 und zum ersten Mal bis 15. Juli 2027. Die zu übermittelnden Informationen werden in einer Verwaltungsvorschrift festgelegt.	

	(7)	(7)Die Berichte nach Absatz 1, Absatz 2 und Absatz 3 dürfen keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Betreiber kritischer Anlagen führen können sowie Handels- oder Geschäftsgeheimnisse enthalten.	
§16		Ermächtigung zum Erlass von Rechtsverordnungen	
	(1)	(1)Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreibern kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter Festlegung der in § 4 Absatz 1 genannten Sektoren wegen ihrer Bedeutung als kritisch geltenden Dienstleistungen und deren als bedeutend geltenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Im Übrigen ist der nach Satz 1 als bedeutend anzusehende Versorgungsgrad anhand von branchenspezifischen Schwellenwerten für jede als kritisch anzusehende Dienstleistung zu bestimmen. In der Rechtsverordnung werden auch Stichtage festgelegt. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	
	(2)	(2)Das Bundesministerium für Wirtschaft und Klimaschutz, das Bundesministerium für Ernährung und Landwirtschaft, das Bundesministerium für Gesundheit, das Bundesministerium für Digitales und Verkehr und das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz werden ermächtigt, im Einvernehmen mit dem Bundesministerium des Innern und für Heimat, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen ihrer jeweiligen Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 konkretisieren. Das Bundesministerium des Innern und für Heimat wird ebenfalls ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen seiner Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 sektorspezifisch konkretisieren.	<p>Es sollten sowohl auf sektorübergreifende als auch sektorspezifische Maßnahmenvorgaben verzichtet werden.</p> <p>Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben.</p> <p>Sollte diese Vorgaben doch durch die zuständigen Behörden erstellt werden, sehen wir eine Beteiligung der Wirtschaft als zwingend erforderlich!</p>
§17		Ausnahmenbescheid	
	(1)	(1)Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums der Justiz, des Bundesministeriums der Verteidigung oder auf eigenes Betreiben Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise befreien (einfacher Ausnahmenbescheid) oder nach Maßgabe des Absatzes 3 insgesamt befreien (erweiterter Ausnahmenbescheid), sofern der Betreiber kritischer Anlagen Vorgaben erfüllt, die den Verpflichtungen nach diesem Gesetz gleichwertig sind. Die Entscheidung nach Satz 1 erfolgt im Benehmen mit dem jeweils zuständigen Ministerium des Bundes oder eines Landes.	
	(2)	(2)Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung, die 1.in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten tätig sind oder Dienste erbringen oder 2.ausschließlich für Behörden, die Aufgaben in relevanten Bereichen nach Nummer 1 erfüllen, tätig sind oder Dienste erbringen. können für diese Tätigkeiten oder Dienste von den Maßnahmen nach §§ 9 bis 12 befreit werden. Die Stärkung der Resilienz muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.	
	(3)	(3)Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung, die ausschließlich in relevanten Bereichen tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von den Registrierungspflichten nach § 6 befreit werden. Absatz 2 Satz 2 gilt entsprechend.	
	(4)	(4)Ein Ausnahmenbescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von Satz 1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Absatzes 2 Satz 1 Nummer 1 oder Nummer 2 von einem Widerruf abgesehen werden.	
§18		Verarbeitung personenbezogener Daten	
	(1)	(1)Die Verarbeitung personenbezogener Daten durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundesamt für Sicherheit in der Informationstechnik, die Bundesnetzagentur, die Bundesanstalt für Finanzdienstleistungsaufsicht sowie durch die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die zuständigen Behörden der Länder nach § 3 Absatz 5 nach diesem Gesetz ist zulässig, soweit 1.dies zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich und 2.eine Verarbeitung anonymisierter oder künstlich erzeugter Daten hierfür nicht in gleicher Weise geeignet ist	
	(2)	(2)Die Verarbeitung personenbezogener Daten durch die in Absatz 1 genannten Behörden zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von § 23 des Bundesdatenschutzgesetzes zulässig, 1.wenn die Verarbeitung erforderlich ist zur a)Sammlung, Auswertung oder Untersuchung von Informationen über nach § 12 gemeldete Vorfälle oder b)zur Unterstützung oder Beratung von Betreibern kritischer Anlagen bei der Gewährleistung ihrer Resilienz und 2.wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.	
	(3)	(3)Die in Absatz 1 Satz 1 genannten Behörden sehen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.	
§19		Bußgeldvorschriften	
	(1)	(1)Ordnungswidrig handelt, wer 1.entgegen § 6 Absatz 1 eine kritische Anlage nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig registriert; 2.entgegen § 6 Absatz 2 dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe auf Verlangen die erforderlichen Aufzeichnungen, Schriftstücke und sonstige Unterlagen nicht vorlegt und Auskunft erteilt; 3.entgegen § 9 Absatz 1 Risikoanalysen und Risikobewertungen nicht oder nicht rechtzeitig durchführt; 4.entgegen § 10 Absatz 1 geeignete und verhältnismäßige Resilienzmaßnahmen nicht oder nicht rechtzeitig trifft; 5.entgegen § 10 Absatz 9 die Maßnahmen nach § 10 Absatz 1 nicht in einem Resilienzplan darstellt und diesen nicht anwendet; 6.entgegen § 11 Absatz 2 Satz 1 weitere Informationen und geeignete Nachweise zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 nicht übersendet; 7.entgegen § 11 Absatz 2 Satz 2 den Resilienzplan und einen geeigneten Nachweis zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 nicht vorlegt; 8.entgegen § 11 Absatz 3 Satz 2 die Ergebnisse der durchgeführten Audits nicht auf Anforderung vorlegt; 9.entgegen § 11 Absatz 3 Satz 3 die Dokumentation, die der Überprüfung durch einen Audit oder auf andere Weise zugrunde gelegt wurde, nicht vorlegt; 10.entgegen § 11 Absatz 5 Satz 3 das Betreten eines Geschäftsraums oder Betriebsraums nicht gestattet, eine Aufzeichnung, ein Schriftstück oder eine Unterlage nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig vorlegt oder eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt; 11.entgegen § 11 Absatz 6 einen geeigneten Mängelbeseitigungsplan nicht oder nicht rechtzeitig vorlegt und Maßnahmen zur Beseitigung der Mängel nicht oder nicht rechtzeitig trifft.	
	(2)	(2)Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist jeweils das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die jeweils zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die jeweils zuständige Behörde der Länder nach § 3 Absatz 5.	
	(3)	(3)Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu [...] Euro geahndet werden.	<p>Der UP KRITIS schlägt vor, bis zur ersten regulären Evaluierung die Bußgelder auszusetzen, zumindest aber den Ansatz zur Bußgeldhöhe des IT-SIG 1.0 zu wählen und nicht den des NIS2UmCG.</p>
§20		Evaluierung	
		Das Bundesministerium des Innern und für Heimat wird die Regelungen dieses Gesetzes regelmäßig, spätestens nach Ablauf von fünf Jahren nach Inkrafttreten des Gesetzes auf wissenschaftlich fundierter Grundlage evaluieren.	<p>Bei der Evaluierung sollten die Branchenverbände zwingend mit einbezogen und auch genügend Zeit zur Verfügung gestellt werden. Die Einbeziehung der Wirtschaft sollte gleichzeitig mit der wissenschaftliche Betrachtung starten. Diese Beteiligung soll nicht die notwendige Verbändeanhörung ersetzen.</p>
		Artikel 2	
		Änderung des Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)	
		Das Dachgesetz zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) vom [...] wird wie folgt geändert. 1.Nach § 10 Absatz 6 wird ein neuer Absatz 7 angefügt: „Die Landesregierungen werden ermächtigt, im Benehmen mit dem Bundesministerium des Innern und für Heimat durch Rechtsverordnung sektorspezifische Mindestvorgaben für Resilienzmaßnahmen nach § 10 Absatz 1 festzulegen, solange und soweit kein entsprechender branchenspezifischer Resilienzenstandard gemäß § 10 Absatz 6 Satz 2 durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe als geeignet anerkannt wurde.“ 2.Absatz 7 wird zu Absatz 8. 3.Absatz 8 wird zu Absatz 9. 4.Absatz 9 wird zu Absatz 10. 5.Absatz 10 wird zu Absatz 11.	
		Artikel 3	
		Inkrafttreten	
(1)		(1)Artikel 1 tritt vorbehaltlich der Absätze 2 und 3 am 18. Oktober 2024 in Kraft.	

(2)	(2) §§ 6, 7, 9 bis 12, 13 Absatz 2, §§ 14, 17 und 19 des Artikel 1 treten am 17. Juli 2026 in Kraft .	In der Erklärung auf Seite 74 des Referentenentwurfes, ist auch die Inkraftsetzung des §16 auf den 17.07.2026 terminiert, auch sonst stimmen die Daten hier nicht übereinander: "Die §§ 6 bis 8, §§ 10 bis 12 und § 16 in Artikel 1 treten abweichend von Absatz 1 am 17. Juli 2026 in Kraft Vor dem Hintergrund, dass zur Erstellung der KRITIS-VO die Erkenntnisse aus den nationalen Risikoanalysen vorliegen müssen, gehen wir davon aus, dass der 17.07.2026 ein realistisches Datum für die Veröffentlichung der KRITIS-VO ist.
(3)	(3) § 19 Absatz 1 Nr. 5 bis 12 des Artikel 1 treten am Werktag auf den folgen-den Tag in Kraft, nachdem das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die jeweiligen branchenspezifische Resilienzstandards nach § 10 Absatz 6 als ge-eignet zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 festgelegt hat, frühestens jedoch am 17. Juli 2026 .	
(4)	(4) Artikel 2 tritt am 01. Januar 2029 in Kraft .	
Begründung		
A. Allgemeiner Teil		
I.	I. Zielsetzung und Notwendigkeit der Regelungen	
	<p>Das KRITIS-DachG wird im Hinblick auf physische Maßnahmen zur Stärkung der Resilienz kritischer Anlagen erstmals einheitliche bundesgesetzliche sektorenübergreifende Mindest-standards normieren.</p> <p>Der Schutz der IT-Sicherheit Kritischer Infrastrukturen ist bereits im Gesetz über das Bun-desamt für Sicherheit in der Informationstechnik (BSiG) niedergelegt. Durch die Umsetzung der NIS-2-Richtlinie mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und durch die DORA-Verordnung werden die Regelungen zum Cyber-schutz von kritischen Infrastrukturen weiterentwickelt. Das KRITIS-DachG wird neben diese Regelungen treten, aber gleichzeitig eine größtmögliche Kohärenz mit den künftigen Rege-lungen im Bereich der IT-Sicherheit von kritischen Anlagen und weiteren Einrichtungen vor-sehen, indem die Schnittstellen zwischen den Bereichen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt werden.</p> <p>Damit wird ein kohärentes System zur Stärkung der Resilienz von Betreibern kritischer An-lagen und weiterer Einrichtungen mit Blick auf physische Maßnahmen und Cyberschutz-maßnahmen geschaffen, welches die jeweiligen europarechtlichen Vorgaben umsetzt.</p> <p>Zu beachten ist dabei, dass beim Cyberschutz bei der Umsetzung der NIS-2-Richtlinie das bereits umfassend bestehende Regelungswerk erweitert wird, während im Hinblick auf phy-sische Resilienzmaßnahmen mit der Umsetzung der Richtlinie (EU) 2022/2557 erstmals umfassende Regelungen getroffen werden. Daher ist die Reichweite des KRITIS-DachG geringer als die Reichweite der Regelungen zur Umsetzung der NIS-2-Richtlinie, die bereits auf ein existierendes Regulationssystem aufsetzt und dieses weiterentwickelt.</p> <p>Die im KRITIS-DachG getroffenen Bestimmungen zu kritischen Anlagen orientieren sich an den bisherigen Regelungen zum Cyberschutz von kritischen Infrastrukturen unter Berücksichtigung der geplanten Umsetzung der NIS-2-Richtlinie, um den Aufbau des Systems unter dem All-Gefahren-Ansatz auch für die Wirtschaft zu erleichtern.</p> <p>Für eine bessere Übersichtlichkeit wird es eine gemeinsame Rechtsverordnung zur Be-stimmung von Betreibern kritischer Anlagen sowie wichtiger und besonders wichtiger Ein-richtungen nach dem KRITIS-DachG und dem BSiG geben. Mit der Rechtsverordnung wird ersichtlich, welche Verpflichtungen für Betreiber von kritischen Anlagen und wichtigen und besonders wichtigen Einrichtungen im Hinblick auf physische Resilienzmaßnahmen nach dem KRITIS-DachG und im Hinblick auf den Cyberschutz nach BSiG gelten. Darüber hin-aus wird für die Registrierung der Betreiber sowie für die Meldung von Störungen eine ge-meinsame technische Lösung angestrebt, sodass hier möglichst geringer Verwaltungsauf-wand für die Wirtschaft entsteht. Die enge Zusammenarbeit der beteiligten Behörden ist überdies im KRITIS-DachG und im BSiG geregelt. Weitere Angleichungen zwischen den Regelungen dieses Gesetzes und den Regelungen des Cyberschutzes werden nach der in § 18 vorgesehenen Evaluierung angestrebt.</p> <p>Das KRITIS-DachG verfolgt in erster Linie den Ansatz, Betreibern kritischer Anlagen kon-krete Vorgaben zur Aufrechterhaltung, Stärkung oder Herstellung ihrer Handlungsfähigkeit und Resilienz zu machen, um dem Risiko einer Beeinträchtigung ihres Geschäftsbetriebs entgegenzuwirken, damit dieser auch bei Störungen oder Ausfällen aufrechterhalten oder schnell wiederhergestellt werden kann. Geregelt werden damit Vorgaben, die präventiv zur Risikovor-sorge in</p>	
II.	II. Wesentlicher Inhalt des Entwurfs	
	<p>Die unionsrechtlichen Vorgaben der Richtlinie (EU) 2022/2557 werden mit dem vorliegen-den Gesetz umgesetzt. Folgende Regelungen werden neu geschaffen:</p> <ul style="list-style-type: none"> -Vorgaben zur Identifizierung von Betreibern kritischer Anlagen und kritischen Ein-richtungen mit besonderer Bedeutung für Europa. -Vorgaben zur Registrierung von Betreibern kritischer Anlagen. -Etablierung von nationalen Risikoanalysen und Risikobewertungen für kritische Dienstleistungen. -Gesetzliche Verankerung wesentlicher nationaler Anforderungen für Resilienzmaß-nahmen von Betreibern kritischer Anlagen. -Einführung eines Meldewesens für Vorfälle. -Umsetzung einer Ausschlussklausel für Betreiber kritischer Anlagen, die einen be-sonderen Bezug zum Sicherheits- und Verteidigungsbereich aufweisen. Für solche Betreiber kritischer Anlagen gelten dann die jeweils einschlägigen Vorgaben für den Sicherheits- bzw. Verteidigungsbereich. -Einführung von Bußgeldvorschriften. 	
III.	III. Alternativen	
	Keine.	
IV	IV. Gesetzgebungskompetenz	
	<p>Die Gesetzgebungskompetenz des Bundes für das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und für die Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-DachG) folgt aus Artikel 74 Absatz 1 Nr. 11 (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 Grundgesetz (GG). Das Recht der Wirtschaft umfasst grundsätzlich alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln und alle Vorschriften, die sich in irgendeiner Form auf die Erzeugung, Herstellung und Verteilung von Gütern des wirtschaftlichen Bedarfs beziehen (z.B. BVerfGE 8, 143, 148 f.). Die Zu-ständigkeit erfasst das öffentliche und das private Wirtschaftsrecht, also auch die wirtschaft-liche Betätigung der öffentlichen Hand.</p> <p>Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Land-gesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die so-wohl im Interesse des Bundes als auch im Interesse der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Be-handlungen gleicher Lebenssachverhalte (zum Beispiel unterschiedliche Anforderungen an die von den Betreibern von kritischen Anlagen zu treffenden Maßnahmen) erhebliche Wett-bewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstä-tigkeit zur Folge hätten.</p> <p>Für den Sektor „Öffentliche Verwaltung“ des Bundes sowie für die Regelung zur nationalen Resilienzstrategie ergibt sich die Gesetzgebungskompetenz des Bundes aus der Natur der Sache.</p> <p>Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).</p>	
V	V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen	
	<p>Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar. Er dient in weiten Teilen der Umsetzung der Richtlinie (EU) 2022/2557.</p> <p>Der Gesetzentwurf ist mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.</p>	
VI	VI. Gesetzesfolgen	
	<p>1. Rechts- und Verwaltungsvereinfachung</p> <p>Der Gesetzesentwurf trägt zur Rechts- und Verwaltungsvereinfachung bei, da er erstmalig bundeseinheitliche Betreiber kritischer Anlagen identifiziert und sektorenübergreifende Vor-gaben für physische Resilienzmaßnahmen schaffen wird, um bestehende Lücken zu schließen. Bei Wahrung der verfassungsgerechten Zuständigkeiten der Aufsichtsbehörden auf Bundes- und Landesebene in den einzelnen Sektoren wird das BSK eine koordinie-rende Rolle erhalten, damit auch im Bereich der physischen Sicherheit ein sektorenüber-greifender Überblick über das Gesamtsystem der Betreiber kritischer Anlagen als einen wesentlichen Teilbereich der kritischen Infrastrukturen geschaffen wird.</p>	
	<p>2. Nachhaltigkeitsaspekte</p> <p>Der Gesetzentwurf ist konform zu dem Leitprinzip der Bundesregierung einer nachhaltigen Entwicklung hinsichtlich des Aufbaus und der Förderung einer widerstandsfähigen Infra-struktur sowie der Sicherung von Lebensqualität und sozialem Zusammenhalt. Er kommt zudem dem Leitgedanken der Bundesregierung zur Berücksichtigung der Nachhaltigkeit nach. Das Einführen bundeseinheitlicher Vorgaben für die Identifizierung von Betreibern kritischer Anlagen sowie Mindestvorgaben für den physischen Schutz fördert eine Stärkung von Lebensqualität durch die Schaffung eines hohen Niveaus an Sicherheit und Resilienz. So ist es im Sinne der Deutschen Nachhaltigkeitsstrategie ein hohes Maß an Versorgungs-sicherheit für die Bürgerinnen und Bürger zu gewährleisten und den sozialen Zusammen-halt und gleichberechtigte Teilhabe an der wirtschaftlichen Entwicklung zu gewährleisten, dem dieser Gesetzentwurf nachkommt. Eine Prüfung der Prinzipien der nachhaltigen Ent-wicklung im Hinblick auf die Nachhaltigkeit wurde vorgenommen: Der Gesetzentwurf ent-spricht in seinen Wirkungen insbesondere den SDG-Indikatoren 3, 8 und 9, deren Ziel der Aufbau und die Förderung einer widerstandsfähigen Infrastruktur ist, sowie ein dauerhaftes, breitenwirksames und nachhaltiges Wirtschaftswachstum und ein gesundes Leben für alle Menschen jeden Alters zu gewährleisten und ihr Wohlergehen zu fördern. Behinderungen etwaiger Nachhaltigkeitsziele durch den Gesetzentwurf wurden nicht fest-gestellt.</p> <p>3. Haushaltsausgaben ohne Erfüllungsaufwand</p> <p>Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen ist finanziell und stellenmäßige im Gesamthaushalt auszugleichen.</p>	

	<p>4.Erfüllungsaufwand</p> <p>Der Regelungsentwurf normiert zahlreiche neue Vorgaben für Wirtschaft und Verwaltung, die erheblichen Erfüllungsaufwand verursachen werden. Dabei haben die Verordnungsermächtigungen gemäß § 16 KRITIS-DachG einen entscheidenden Einfluss darauf, wie viele Unternehmen und Bundesbehörden in den Anwendungsbereich zur Stärkung der physischen Resilienz fallen werden und welche konkreten Maßnahmen diese zur Erfüllung einzelner Vorgaben durchführen müssen. Spiegebildlich werden dadurch auch Aufwände der Vollzugsbehörden der Länder und des Bundes beeinflusst, da Aufwände aus vielen Vorgaben von der Anzahl der in den Anwendungsbereich fallenden Unternehmen und Behörden abhängig sind.</p> <p>Die nachfolgende Schätzung zum KRITIS-DachG beziffert ausschließlich den Erfüllungsaufwand aus Vorgaben, deren Erfüllung nicht oder nur unwesentlich durch die Verordnungsermächtigung beeinflusst wird. Der Erfüllungsaufwand der übrigen Vorgaben wird bei der Ausarbeitung der Rechtsverordnungen geschätzt.</p> <p>a.Erfüllungsaufwand für die Bürgerinnen und Bürger</p> <p>Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.</p> <p>b.Erfüllungsaufwand für die Wirtschaft</p> <p>Der Erfüllungsaufwand aus jeder Vorgabe ist direkt oder indirekt abhängig von der Anzahl der Betreiber kritischer Anlagen (vgl. Tabelle). Diese Anzahl kann erst ermittelt werden, wenn durch § 16 Absatz 1 KRITIS-DachG konkret bestimmt wird, welche Anlagen kritische Anlagen im Sinne des KRITIS-DachG sind. Zudem werden bei vielen Vorgaben der Zeitaufwand und/oder die Sachkosten direkt oder indirekt durch die sektorspezifischen Mindestanforderungen beeinflusst, die durch die Rechtsverordnung gemäß § 16 Absatz 2 KRITIS-DachG bestimmt werden. Ohne die Konkretisierungen der Rechtsverordnungen ist eine verlässliche Schätzung des Erfüllungsaufwands nicht möglich.</p> <p>Lfd-Nr.Paragraph und Normbezeichnung der Vorgabefallzahl*Zeitaufwand/Sachkosten pro Fall**Darstellung der Schätzung in...</p> <p>Zb.15§ 6 und 7 KRITIS-DachG-Eregistrierungs- und Meldepflicht Verordnung</p> <p>Zb.2§ 9 KRITIS-DachG-Durchführung von Risikoanalysen und Risikobewertung Verordnung</p> <p>Zb.3§ 10 Absätze 1 und 2 sowie § 14 KRITIS-DachG-Einhaltung eines Mindestniveaus an physischer Resilienz Verordnung</p> <p>Zb.4§ 10 Absatz 6 KRITIS-DachG-Antrag zur Genehmigung branchenspezifischer Standards Verordnung</p> <p>Zb.5§ 10 Absatz 7 KRITIS-DachG-Erarbeitung von Resilienzplänen Verordnung</p> <p>Zb.6§ 11 KRITIS-DachG-ENachweis über Einhaltung eines Mindestniveaus an physischer Resilienz Verordnung</p> <p>Zb.7§ 9 bis 11 in Verbindung mit § 4 Absatz 7 KRITIS-DachG-Antrag auf Äquivalenzprüfung Verordnung</p> <p>Zb.8§ 12 KRITIS-DachG-Emeldung von Sicherheitsvorfällen Verordnung</p>	
	<p>Für eine erste Einordnung hat das Statistische Bundesamt eine erste Einschätzung vorgenommen: Vorgabe Zb.3 wird mit Abstand den größten Aufwand verursachen. Das Bundesamt hat für eine erste Annäherung eine sehr grobe Schätzung des Erfüllungsaufwands vorgenommen. Ohne Informationen von Expertinnen und Experten zu Aufwänden von notwendigen Maßnahmen zur Stärkung der physischen Resilienz hat es die Kosten auf Basis von Ausgaben zur IT-Sicherheit aus Vorgaben des IT-Sicherheitsgesetzes und des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 geschätzt. Unter den sehr vereinfachten Annahmen, dass Kosten aus Vorgaben zur physischen Resilienz zehn Mal so hoch sind wie Kosten aus Vorgaben zur IT-Sicherheit und dass Anlagen von rund 1 300 Betreibern kritischer Anlagen über keine ausreichende physische Resilienz verfügen, verursachen die Vorgaben des Regelungsentwurfs vermutlich einen jährlichen Erfüllungsaufwand im hohen dreistelligen Millionenbereich. Das Statistische Bundesamt weist darauf hin, dass eine solche Schätzung nur eine ungefähre Einordnung darstellt, welchen Umfang die Kosten haben können. Die Kosten können geringer, aber auch wesentlich höher sein. Eine belastbare Schätzung ist erst dann möglich, wenn die allgemeinen Vorgaben des KRITIS-DachG durch die Rechtsverordnungen konkretisiert werden und hierzu Experteneinschätzungen vorliegen.</p> <p>Auf Basis der langjährigen Erfahrung aus der Nachmessung des Erfüllungsaufwands schätzt das Bundesamt, dass die Vorgaben Nummern Zb.1, Zb.4 bis Zb.8 relativ geringen jährlichen Erfüllungsaufwand verursachen werden. Angaben aus dem Impact assessment (vgl. S. ...) weisen darauf hin, dass aus Vorgabe Zb.2 spürbarer jährlicher Erfüllungsaufwand im einstelligen Millionenbereich entstehen kann.</p>	
	<p>c.Erfüllungsaufwand für die Verwaltung</p> <p>Der Bundes- und Landesverwaltung entsteht Erfüllungsaufwand aus dem Vollzug des KRITIS-DachG (vgl. Tabelle, Vorgaben Zc.1 bis Zc.12). Zudem müssen bestimmte Bundesbehörden – ähnlich wie die Betreiber kritischer Anlagen – Maßnahmen zur Sicherung der physischen Resilienz ergreifen (vgl. Tabelle, Vorgaben Zc.13 bis Zc.19).</p> <p>.....</p> <p>Zc.5 § 10 Absätze 4 bis 6 und 8 KRITIS-DachG-Esektorenübergreifende Mindestanforderungen und branchenspezifische ResilienzstandardsBBK, BSI, BMI und Bundes- und Landesbehörden nach § 3</p> <p>.....</p>	<p>Es sollen sich auf Bundesebene 29 Vollzeitstellen mit dem Nachweisverfahren beschäftigen; dazu kommen noch geschätzte 17,4 Stellen auf Landesebene.</p> <p>Sollte dem Vorschlag des UP KRITIS Folge geleistet werden, sind zumindest in den Jahren bis zur Evaluierung diese Stellen nicht in diesem Umfang notwendig. Stichproben können durch wesentlich weniger Personalressourcen gemacht werden und Erkenntnisse aus den Stichproben können dann in die Evaluierung einfließen.</p>
	<p>5.Weitere Kosten</p> <p>Keine.</p>	
	<p>6.Weitere Gesetzesfolgen</p> <p>Durch den Gesetzesentwurf wird die Versorgungssicherheit für Verbraucherinnen und Verbraucher erhöht. Die Regelungen des Gesetzesentwurfs sind inhaltlich geschlechtsneutral aufgrund der vorrangig gegebenen unmittelbaren Betroffenheit der Zielgruppe des Regelungsvorhabens und damit ohne Gleichstellungsrelevanz. Die weitere Stärkung und Förderung im Bereich des physischen Schutzes von Betreibern kritischer Anlagen betrifft jedoch sowohl mittel- als auch unmittelbar Frauen und Männer. § 1 Absatz 2 des Bundesgleichstellungsgesetzes bestimmt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Dies wurde in der Entwicklung der Gesetzesformulierung unter Einbeziehung bereits gegebener Diktion berücksichtigt.</p> <p>Die Regelungen entsprechen zudem den Anforderungen des „Gleichwertigkeits-Checks“. Der Gesetzesentwurf dient der Versorgungssicherheit der Bevölkerung durch Stärkung der Resilienz von kritischen Anlagen. Auch wird dem Schutz einer Daseinsvorsorge mit ihren unterschiedlichen Bereichen, die eine wesentliche Voraussetzung für gleichwertige Lebensverhältnisse der Menschen und den gesellschaftlichen Zusammenhalt Rechnung getragen. Auswirkungen auf die vorhandene Siedlungs- und Raumstruktur oder demographische Belange sind nicht zu erwarten.</p>	
	<p>VII. VII.Befristung: Evaluierung</p>	
	<p>Eine Befristung ist nicht vorgesehen, da das Gesetz der Umsetzung der Richtlinie (EU) 2022/2557 dient, die unbefristet gilt. Das Gesetz soll anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Beschluss des Staatssekretärausschusses Bessere Rechtsetzung und Bürokratieabbau vom 23. Januar 2013 maximal fünf Jahre nach Inkrafttreten der jeweils evaluierungsbedürftigen Regelungen evaluiert werden.</p> <p>§ 19 sieht dazu eine Evaluierungsklausel vor. Auf die Begründung zu § 19 wird verwiesen.</p>	
B.	Besonderer Teil	
	<p>Zu Artikel 1 (Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen)</p>	
	<p>Zu § 1 (Nationale KRITIS-Resilienzstrategie)</p> <p>Die Vorschrift dient der Umsetzung von Artikel 4 der Richtlinie (EU) 2022/2557. Bis 17. Januar 2026 muss die Bundesregierung eine nationale Strategie zur Verbesserung der Resilienz von Betreibern kritischer Anlagen verabschieden. In dieser Strategie sollen die strategischen Ziele und politischen Maßnahmen festgelegt werden, mit denen ein hohes Resilienz-niveau von Betreibern kritischer Anlagen erreicht und aufrechterhalten werden soll. Die Strategie soll gemeinsam mit den Ländern und unter Beteiligung der Zivilgesellschaft erarbeitet werden und die Strategie der Bundesregierung zum Schutz Kritischer Infrastrukturen von 2019 aktualisieren.</p>	
	<p>Zu § 2 (Begriffsbestimmungen)</p> <p>Zu Nummer 1</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 1 der Richtlinie (EU) 2022/2557. Der in der Richtlinie verwendete Begriff der „kritischen Einrichtung“ wird im Hinblick auf den in Deutschland etablierten Bezug zu Anlagen und Anlagenkategorien mit dem Begriff „Betreiber kritischer Anlagen“ umgesetzt. Die nähere Bestimmung von Betreibern kritischer Anlagen erfolgt nach § 4 in Verbindung mit der Rechtsverordnung nach § 16 Absatz 1. Die Rechtsverordnung nach § 16 Absatz 1 wird die Einrichtungskategorien gemäß der dritten Spalte der Tabelle im Anhang zur Richtlinie (EU) 2022/2557 berücksichtigen.</p> <p>Zu Nummer 2</p> <p>Eine Anlage ist eine Betriebsstätte, sonstige ortsfeste Installation, Maschine, Gerät und sonstige ortsveränderliche technische Installation.</p> <p>Zu Nummer 3</p> <p>Eine kritische Anlage ist eine Anlage nach § 3 Nr. 2, die für eine kritische Dienstleistung nach § 2 Nr. 4 notwendig ist.</p> <p>Zu Nummer 4</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 5 der Richtlinie (EU) 2022/2557. Statt des Begriffs der „wesentlichen Dienste“ wird der in der Fachpraxis etablierte Begriff der „kritischen Dienstleistung“ verwendet. Die Rechtsverordnung nach § 16 Absatz 1 wird eine Auflistung der kritischen Dienstleistungen enthalten, die die Delegierte Verordnung (EU) 2023/2450 der Kommission vom 25. Juli 2023 zur Ergänzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste berücksichtigt.</p> <p>Zu Nummer 5</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 2 der Richtlinie (EU) 2022/2557.</p> <p>Zu Nummer 6</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 6 der Richtlinie (EU) 2022/2557.</p> <p>Zu Nummer 7</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 2 Nr. 7 der Richtlinie (EU) 2022/2557. Zwar lässt sich der Begriff „Risikoanalyse“ in der Form, wie er in diesem Gesetz verwendet wird, in der Richtlinie (EU) 2022/2557 nicht finden. Die Richtlinie (EU) 2022/2557 verwendet unter Artikel 2 Nr. 7 insgesamt den Begriff der „Risikobewertung“. Im deutschen Sprach- und Rechtsgebrauch wird der Begriff „Risikobewertung“ jedoch enger gefasst. Während der Begriff „Risikobewertung“ im deutschen Sprachgebrauch der in diesem Gesetz definierten Beschreibung entspricht („Prozess der Priorisierung und des Vergleichs von Risiken“), geht der Begriff in der Richtlinie (EU) 2022/2557 weiter und nimmt noch den Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos auf, also das, was im deutschen Sprachgebrauch unter „Risikoanalyse“ verstanden wird. Diese weitergehende Begriffsbestimmung wird daher in diesem Gesetz</p>	

	<p>Zu § 3 (Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit)</p> <p>Zu Absatz 1</p> <p>§ 3 Absatz 1 regelt, dass das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zentrale Anlaufstelle i.S.d. Artikel 9 Absatz 2 der Richtlinie (EU) 2022/2557 ist.</p> <p>Gemäß Artikel 9 Absatz 2 der Richtlinie (EU) 2022/2557 muss jeder Mitgliedstaat eine zentrale Anlaufstelle benennen oder einrichten, die als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zentralen Anlaufstellen anderer Mitgliedstaaten und mit der in Artikel 19 der Richtlinie (EU) 2022/2557 genannten Gruppe für die Resilienz kritischer Einrichtungen fungiert. Die Errichtung und Benennung einer solchen dient der Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation sowie Koordinierung von Fragen im Zusammenhang mit der Resilienz kritischer Einrichtungen.</p> <p>Als zentrale Anlaufstelle wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Geschäftsbereich des Bundesministeriums des Innern und für Heimat benannt. Hierdurch wird zum einen eine effektive Umsetzung der Richtlinie (EU) 2022/2557 gewährleistet.</p> <p>Zu Absatz 2</p> <p>Gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2557 werden die Mitgliedstaaten verpflichtet, eine oder mehrere Behörden zu ernennen oder einzurichten, die für die Überwachung und gegebenenfalls die Durchsetzung von Bestimmungen dieser Richtlinie zuständig sind.</p> <p>Zuständige Behörden sind im Hinblick auf Zuständigkeiten des Bundes das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, in Bezug auf öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste die Bundesnetzagentur und für alle anderen Betreiber kritischer Anlagen im Sektor Informationstechnik und Telekommunikation das Bundesamt für Sicherheit in der Informationstechnik, in Bezug auf den Sektor Finanz- und Versicherungswesen die Bundesanstalt für Finanzdienstleistungsaufsicht sowie die weiteren Aufsichtsbehörden des Bundes nach Absatz 3 und im Hinblick auf Zuständigkeiten der Länder die zuständigen Landesbehörden nach Absatz 5.</p> <p>Zu Absatz 3</p> <p>Das sektorspezifische Fachwissen für die verschiedenen Sektoren befindet sich teilweise in Bundeszuständigkeit und teilweise in Länderzuständigkeit. Um dieses sektorspezifische Fachwissen beim Vollzug des KRITIS-Dachgesetzes vollumfänglich nutzen zu können, werden Aufgaben des KRITIS-DachG je nach Bundes- oder Länderzuständigkeit den entsprechenden Behörden zugeteilt. Zur deutlichen Abgrenzung werden in Absatz 3 die Zuständigkeiten des Bundes in Bezug auf kritische Dienstleistungen ausdrücklich benannt. Es handelt sich um einen Teilbereich der kritischen Dienstleistungen, für die die Verpflichtungen des KRITIS-DachG gelten und die in der Rechtsverordnung nach § 16 Absatz 1 benannt werden. Bei den in Absatz 3 nicht genannten kritischen Dienstleistungen handelt es sich um Zuständigkeiten der Länder.</p> <p>Das Bundesministerium des Innern und für Heimat macht die zuständigen Bundesbehörden im Bundesanzeiger bekannt.</p>	<p>Zu Absatz 2: Hier wird nicht der Energiesektor benannt, wobei die Aufsichtspflicht ja bei der BNetzA liegt?</p> <p>Zu Absatz 5: Hier sind dann die zuständigen sektorspezifischen Landesbehörden adressiert. Somit gibt es zukünftig eine zentrale koordinierende Bundesbehörde, dazu "n" sektorspezifische Bundesbehörden, 16 zentrale Landesbehörden, und "n" sektorspezifische Landesbehörden aus 16 Bundesländern. Für ein Unternehmen, das in mehreren Bundesländern kritische Dienstleistungen erbringt, käme zu "bedienen"!</p>
	<p>Zu § 4 (Anwendungsbereich; kritische Anlagen; Geltungsbereich)</p> <p>Zu Absatz 1</p> <p>§ 4 definiert den Anwendungsbereich des KRITIS-DachG. In Umsetzung der Richtlinie (EU) 2022/2557 werden Betreiber kritischer Anlagen in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation und Weltraum ermittelt. Zusätzlich werden Betreiber kritischer Anlagen im Sektor Siedlungsabfallentsorgung ermittelt. Dieser Sektor ist bereits gem. § 2 Abs. 10 Nr. 1 BStG als Sektor der kritischen Infrastruktur festgelegt. Im Sinne einer weitgehenden Kohärenz der Adressaten für Vorgaben für den Cyber-schutz und für physische Resilienzmaßnahmen wird dieser Sektor über die Mindestvorgaben der Richtlinie (EU) 2022/2557 in den Anwendungsbereich des vorliegenden Gesetzes aufgenommen. Während der Regelungsbereich für den Cyberschutz ausgeweitet wird, sollen die Resilienzmaßnahmen nach der Richtlinie (EU) 2022/2557 im ersten Schritt nur für einen kleineren Kreis von Betreibern kritischer Anlagen gelten. Die Ausweitung des Anwendungsbereichs wird Gegenstand der in § 20 vorgesehenen Evaluierung.</p> <p>Innerhalb dieser Sektoren sind nur solche Betreiber kritischer Anlagen, die einen oder mehrere kritische Dienstleistungen erbringen, die für das Funktionieren der Gesamtwirtschaft des Gemeinwesens von hoher Bedeutung sind und ein Vorfall eine erhebliche Störung bei der Erbringung eines oder mehrerer kritischer Dienstleistungen durch die Anlage, oder bei der Erbringung von anderen kritischen Dienstleistungen in den im Anhang genannten Sektoren, die von diesen kritischen Dienstleistungen abhängen, bewirken würde.</p> <p>In einer konkretisierenden Rechtsverordnung nach § 16 Absatz 1 wird festgelegt, welche Dienstleistungen überhaupt in den Sektoren als kritisch im Sinne des KRITIS-DachG gelten. Diese Rechtsverordnung orientiert sich systematisch und inhaltlich an der BSI-Kritikverordnung, die im Rahmen der IT-Sicherheit von kritischen Infrastrukturen bisher definiert, welche Anlagen als kritisch eingestuft werden. Demnach liegt aus Bundesicht Kritikalität vor, sofern eine Anlage eine kritische Dienstleistung ausführt und einen in der Rechtsverordnung festgelegten Schwellenwert überschreitet. Der Schwellenwert wird auf Grundlage des Kriteriums der zu versorgenden Bevölkerung berechnet. Dabei soll – ebenso wie in der BSI-Kritikverordnung – grundsätzlich eine zu versorgende Bevölkerung von 500.000 Personen zu Grunde gelegt werden. Sofern eine Anlage eine Bevölkerungszahl von dieser Größe versorgt, wird davon ausgegangen, dass dies aus Bundesicht für die Aufrechterhaltung der Wirtschaft wesentlich ist.</p> <p>Unter Berücksichtigung der dem Bund zustehenden Gesetzgebungskompetenz aus Art. 74 Absatz 1 Nr. 11 GG – dem Recht der Wirtschaft – wird bei der Umsetzung der Richtlinie (EU) 2022/2557 der Schwerpunkt auf das Schutzziel der Aufrechterhaltung der wichtigen wirtschaftlichen Tätigkeiten gelegt. Die im vorliegenden Gesetz enthaltenen Regelungen zur Stärkung der Resilienz bewirken daneben insbesondere auch eine Stärkung der weiteren in der Richtlinie (EU) 2022/2557 genannten Schutzziele der öffentlichen Gesundheit und Sicherheit. Im Hinblick auf den Anwendungsbereich bedeutet dies, dass die Dienstleistung aus Bundesicht für die Aufrechterhaltung wichtiger wirtschaftlicher Tätigkeiten von entscheidender Bedeutung ist.</p> <p>Zugrunde gelegt wird die Betrachtungsebene des Bundes und diejenigen Organisationen und Einrichtungen werden adressiert, von denen auch die kleinen und</p>	<p>Der Anregung, die in der CER-Richtlinie enthaltenen Unterstützungsmaßnahmen (u.a. beschleunigtes ZUP-Verfahren, Vergabe staatlicher Beihilfen) in das KRITIS-DachG aufzunehmen, wurde nicht entsprochen.</p>
	<p>Zu § 5 (Einrichtungen der Bundesverwaltung)</p> <p>Zu Absatz 1</p> <p>Der Anwendungsbereich der Richtlinie (EU) 2022/2557 umfasst gemäß Nr. 9 des Anhangs der Richtlinie (EU) 2022/2557 im Sektor öffentliche Verwaltung Einrichtungen der öffentlichen Verwaltung von Zentralregierungen entsprechend der jeweiligen Definition der Mitgliedstaaten gemäß nationalem Recht. Die Festlegung der Einrichtungen wird im Rahmen der Rechtsverordnung nach § 16 erfolgen. In Anlehnung an die deutsche Definition von „zentrale Regierungsbehörden“ in der Richtlinie 2014/74/EU sollen als „Zentralregierung“ die Bundesministerien und das Bundeskanzleramt ausgenommen der jeweiligen Geschäftsbereichsbehörden gefasst werden.</p> <p>Zu Absatz 2</p> <p>Nach Artikel 1 Absatz 6 der Richtlinie (EU) 2022/2557 gelten die Vorschriften der Richtlinie nicht für Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung – einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten – ausüben. Die Richtlinie soll nicht die Zuständigkeit der Mitgliedstaaten und ihrer Behörden hinsichtlich der Verwaltungsaufonomie oder ihre Verantwortung für den Schutz der nationalen Sicherheit und Verteidigung oder ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, insbesondere in Bezug auf die öffentliche Sicherheit, die territoriale Unversehrtheit und die Aufrechterhaltung der öffentlichen Ordnung berühren. Daher sind die Einrichtungen mit der Bezug im KRITIS-DachG von dem Anwendungsbereich ebenso ausgeschlossen.</p> <p>Zu Absatz 3</p> <p>Für die gemäß der Rechtsverordnung nach § 16 Absatz 1 identifizierten Einrichtungen der Bundesverwaltung sind die Pflichten nach §§ 6, 9, § 10 Absatz 1 bis 5, 7 bis 10, §§ 11 bis 13, 17 und 18 dieses Gesetzes entsprechend anzuwenden. Um die Aufrechterhaltung der Staats- und Regierungsfunktion bei einem Vorfall im Sinne dieses Gesetzes sicherzustellen, unterliegen diese Einrichtungen allen Verpflichtungen, die auch Betreiber kritischer Anlagen in den anderen Sektoren erfüllen müssen.</p> <p>Zu Absatz 4</p> <p>Die Vorschriften für Kritische Einrichtungen mit besonderer Bedeutung für Europa nach § 7 und zur Geschäftsleiterhaftung nach § 14 sind nicht auf Einrichtungen im Sektor öffentliche Verwaltung anzuwenden.</p> <p>Zu Absatz 5</p> <p>Im Einklang mit § 10 Absatz 6 legt Absatz 5 für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die Möglichkeit fest, Standards zu entwickeln, die im Einvernehmen mit den Bundesressorts und dem Bundesamt für Sicherheit in der Informationstechnik festgelegt werden und die Maßnahmen im Hinblick auf § 10 Absatz 1 konkretisieren.</p> <p>Zu Absatz 6</p>	
	<p>Zu § 6 (Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt)</p> <p>Zu Absatz 1</p> <p>Angelehnt an die Registrierungspflicht der Betreiber von Betreibern kritischer Anlagen nach § 8 b Abs. 3 BStG soll eine Registrierung bei einer gemeinsam vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem und dem Bundesamt für Sicherheit in der Informationstechnik eingerichteten Registrierungsmöglichkeit durch die Betreiber selbst erfolgen, um ein kohärentes System zwischen den hiesigen Vorschriften und den Vorschriften des BStG zu schaffen. Auch soll ein zu hoher bürokratischer Aufwand vermieden werden. Unter anderem wird durch die Registrierung auch sichergestellt, dass die Verpflichtungen bzw. Resilienzanforderungen aus diesem Gesetz an die relevanten Betreiber nachvollzogen bzw. überprüft werden können.</p> <p>Zu Absatz 2</p> <p>Die Pflicht der Betreiber kritischer Anlagen zur Vorlage von erforderlichen Aufzeichnungen, Schriftstücken oder sonstigen Unterlagen besteht, um die Registrierungspflicht sicherzustellen. Hierzu benötigt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in begründeten Fällen die Möglichkeit, relevante Informationen von solchen Betreibern kritischer Anlagen zwecks Prüfung zu verlangen, bei denen Tatsachen die Annahme rechtfertigen, dass die Registrierungspflicht nicht erfüllt wurde oder wird. Die Verpflichtung zur Vorlage auf Verlangen ist relevant, damit auch die weitergehenden Anforderungen nach diesem Gesetz nachvollzogen und eingehalten werden können. Der Schutz von Geheimheitsinteressen oder überwiegenden Sicherheitsinteressen dient dabei als gebotene Einschränkung und berücksichtigt Bereiche, in denen die Offenlegung von sensiblen Informationen negative Auswirkungen für den Betrieb der Betreiber kritischer Anlagen oder die Versorgung mit der Betrachtenden kritischen Dienstleistung haben könnte.</p> <p>Zu Absatz 3</p> <p>Ebenfalls in Anlehnung an § 8b Abs. 3 S. 2 BStG kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die Registrierung im Einvernehmen mit den sonst zuständigen Bundesbehörden selbst vornehmen. Im Falle betreiberseitigen Unterlassens der Registrierung trotz Vorliegens der gesetzlichen Verpflichtung hierzu ist behördenseitig – im Einvernehmen mit der zuständigen Behörde – eine Erfassung von Amts wegen zu veranlassen. Hierdurch sollen ebenfalls die Einhaltung und Überprüfung der betreiberseitigen Verpflichtungen aus diesem Gesetz sichergestellt bzw. nachvollzogen werden.</p> <p>Zu Absatz 4</p> <p>Absatz 4 gilt als Klarstellung, dass für die nicht qua Rechtsverordnung, sondern auf Grund des Vorschlagsrechts identifizierten Betreiber kritischer Anlagen die Vorschriften der Registrierung gelten.</p> <p>Zu Absatz 5</p> <p>Die für sie jeweils federführend zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 wird dem Betreiber kritischer Anlagen aus Gründen der Transparenz und Klarheit mitgeteilt.</p> <p>Zu Absatz 6</p>	

	<p>Zu § 7 (Kritische Einrichtungen von besonderer Bedeutung für Europa)</p> <p>Zu Absatz 1</p> <p>Zwar sind Betreiber kritischer Anlagen in der Regel als Teil eines immer stärker vernetzten Dienstleistungs- und Infrastrukturnetzes tätig und erbringen häufig kritische Dienstleistungen in mehr als einem Mitgliedstaat, doch sind einige dieser Betreiber kritischer Anlagen für die Union und ihren Binnenmarkt von besonderer Bedeutung, da sie kritische Dienstleistungen für oder in sechs oder mehr Mitgliedstaaten erbringen und daher eine spezifische Unterstützung auf Unionsebene erhalten sollten. Diese quantitative Voraussetzung und die Mitteilung der Europäischen Kommission identifizieren den Betreiber kritischer Anlagen nach § 4 Absatz 1 als eine kritische Einrichtung mit besonderer Bedeutung für Europa.</p> <p>Zu Absatz 2</p> <p>Der Betreiber kritischer Anlagen hat dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bei Registrierung mitzuteilen, dass kritische Dienstleistungen für oder in mehr als sechs Mitgliedstaaten erbracht werden. Dies beinhaltet die Mitteilung darüber, welche Dienstleistungen er für oder in diesen Mitgliedstaaten anbietet und für welche oder in welchen Mitgliedstaaten diese angeboten werden. Nach Meldung des Betreibers der kritischen Anlage beim BBK, dass es Dienstleistungen nach EU VO [Delegierter Rechtsakt - Liste wesentlicher Dienste] in mindestens sechs Mitgliedstaaten erbracht werden, teilt das BBK der Europäischen Kommission unverzüglich die Identität solcher kritischen Einrichtungen sowie die Informationen, die diese zur Verfügung stellen, mit. Die Europäische Kommission konsultiert das BBK, das eine kritische Einrichtung ermittelt hat, die zuständige Behörde anderer betroffener Mitgliedstaaten sowie die betreffende kritische Einrichtung. Bei diesen Konsultationen teilen die Behörden der Mitgliedstaaten der Europäischen Kommission mit, ob es sich seiner Einschätzung nach bei den Diensten, die diesem Mitgliedstaat von der kritischen Einrichtung erbracht werden, um wesentliche Dienste handelt.</p> <p>Zu Absatz 3</p> <p>Stellt die Kommission auf der Grundlage der Konsultationen fest, dass die betreffende kritische Einrichtung für oder in sechs oder mehr Mitgliedstaaten wesentliche Dienste im Sinne der Delegierten Verordnung (EU) 2023/2450 erbringt, so teilt die Kommission dem Betreiber dieser kritischen Anlage über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mit, dass sie als kritische Einrichtung von besonderer Bedeutung für Europa gilt, und unterrichtet diese über ihre Verpflichtungen gemäß § 6 ff. sowie über den Zeitpunkt, ab dem diese Verpflichtungen für sie gelten. Sobald die Kommission die zuständige Behörde über ihre Entscheidung informiert, eine Einrichtung als kritische Einrichtung von besonderer Bedeutung für Europa zu betrachten, leitet die zuständige Behörde diese Meldung unverzüglich an diese kritische Einrichtung weiter.</p> <p>Diese Vorgaben gelten für die betreffenden kritischen Einrichtungen von besonderer Bedeutung für Europa ab dem Tag des Eingangs der in Absatz 3 genannten Mitteilung.</p> <p>Zu Absatz 4</p> <p>Der Absatz 4 dient der Umsetzung des Artikel 18 der Richtlinie (EU) 2022/2557.</p>	
	<p>Zu § 8 (Nationale Risikoanalysen und Risikobewertungen)</p> <p>Zu Absatz 1</p> <p>Im Einklang mit Art. 5 der Richtlinie (EU) 2022/2557 wird durch § 8 Abs. 1 festgelegt, dass die für die jeweiligen kritischen Dienstleistungen nach § 3 Absatz 3 und 5 zuständigen Bundesministerien und Landesministerien alle vier Jahre oder bei Veranlassung für die auf der Grundlage der Rechtsverordnung nach § 16 bestimmten kritischen Dienstleistungen Risikoanalysen und Risikobewertungen durchführen. Hierbei sind mindestens die in § 8 Abs. 1 Nr. 1 - Nr. 5 gesetzlich vorgegebenen Voraussetzungen zu beachten.</p> <p>Durch regelmäßige Risikoanalysen und Risikobewertungen, die bestehende Analysen und Bewertungen berücksichtigen, sollen Betreiber kritischer Anlagen ermittelt und Betreiber kritischer Anlagen bei der Vornahme von Resilienzmaßnahmen dieses Gesetzes unterstützt werden, sowie die Bedarfe an privaten und staatlichen Schutzmaßnahmen herausgearbeitet werden.</p> <p>Die Maßnahmen sollen einem risikobasierten Ansatz folgen, bei dem diejenigen kritischen Dienstleistungen im Fokus stehen, die für die Erfüllung wichtiger wirtschaftlicher Tätigkeiten mit einem nicht unerheblichen gesellschaftlichen Einfluss am bedeutendsten sind. Für die sen risikobasierten Ansatz müssen natürliche und vom Menschen verursachte Risiken – einschließlich Risiken grenzüberschreitender oder sektorübergreifender Art – analysiert und bewertet werden, die sich auf die Erbringung kritischer Dienstleistungen auswirken könnten. Zu diesen Risiken gehören insbesondere Unfälle, Naturkatastrophen, gesundheitliche Notlagen wie etwa Pandemien und hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, krimineller Unterwanderung und Sabotage. Auch Risiken sektorübergreifender grenzüberschreitender Art sind zu berücksichtigen. Bei der Risikoanalyse und der Risikobewertung sollen die Erkenntnisse anderer thematisch betroffener Fachressorts (z.B. diejenigen der Sicherheitsbehörden) in die Bewertungen mit einfließen.</p> <p>Bei der Durchführung von Risikobewertungen sollten andere allgemeine oder sektorspezifische Risikobewertungen berücksichtigt werden, die gemäß anderer Unionsrechtsakte durchgeführt werden, und das Ausmaß der Abhängigkeit zwischen Sektoren, auch in Bezug auf Sektoren in anderen Mitgliedstaaten und Drittstaaten, Rechnung tragen. Dem tragen vor allem § 8 Nr. 3 und Nr. 4 Rechnung.</p> <p>Zu Absatz 2</p> <p>Die Festlegung methodischer und inhaltlicher Vorgaben durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe folgt der umfangreichen fachlichen, sektorenübergreifenden und methodischen Expertise im Bereich des physischen Schutzes von Betreibern kritischer Anlagen.</p> <p>Zu Absatz 3</p> <p>Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe wertet die nach Absatz 1 durch die Bundesministerien und Landesministerien durchgeführten nationalen Risikoanalysen und Risikobewertungen sektorenübergreifend aus.</p> <p>Zu Absatz 4</p>	<p>Bei feindliche Bedrohungen und vor allem terroristische Straftaten sollten Behörden konkrete behördliche Unterstützungsmaßnahmen für die Wirtschaft festlegen. Kritische Betreiber sollten in Szenarioübungen der Sicherheitsbehörden anlassbezogen eingebunden werden. Die Verantwortlichkeiten und hoheitlichen Befugnisse bei solchen Ad-Hoc-Lagen sollten klar definiert sein.</p> <p>Hierbei ist die Berücksichtigung von neuen Ansätzen bei den speziellen Maßnahmen zu Terrorismus anhand des neuen Referentenentwurfs zur Bekämpfung von Terrorismus (EU) empfehlenswert</p>
	<p>Zu § 9 (Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen)</p> <p>Zu Absatz 1</p> <p>Durch § 9 Absatz 1 wird festgelegt, dass auf Grundlage der nationalen Risikoanalysen und Risikobewertungen nach § 8 dieses Gesetzes Risikoanalysen und Risikobewertungen durch Betreiber kritischer Anlagen durchzuführen sind. Dies dient auch der Umsetzung des Art. 12 der Richtlinie (EU) 2022/2557.</p> <p>Bei der Durchführung sind nach § 9 Abs. 1 die naturbedingten, klimatischen und vom Menschen verursachten Risiken nach § 8 Abs. 1 a) – c) zu berücksichtigen. Darüber hinaus sind nach § 9 Abs. 1 Nr. 2 die die Wirtschaftsstabilität beeinträchtigenden Risiken nach gemäß § 9 Abs. 1 Nr. 2 a) und b) ebenfalls miteinzubeziehen.</p> <p>Hintergrund ist, dass Betreiber kritischer Anlagen die entsprechenden Risiken, denen sie ausgesetzt sind, in ihrer Gesamtheit bekannt sind bzw. werden. Auf dieser Grundlage sollen sie in der Lage sein, geeignete Resilienzmaßnahmen zu treffen. Dazu sieht die Vorschrift vor, Betreiber kritischer Anlagen zu verpflichten, diejenigen Risiken zu analysieren und zu bewerten, die die Aufrechterhaltung ihres Geschäftsbetriebs und damit die Erbringung ihrer kritischen Dienstleistung stören oder unterbrechen können. Als Grundlage dafür sollen die staatlichen Risikoanalysen und -bewertungen nach § 8 dieses Gesetzes dienen. Auch andere Informationsquellen können herangezogen werden. Die Risikoanalyse und -bewertung ist grundsätzlich mindestens alle vier Jahre durchzuführen, erstmalig neun Monate seit Registrierung der kritischen Anlage nach gemäß § 6 Abs. 6 dieses Gesetzes. Darüber hinaus sollen Betreiber kritischer Anlagen eine Risikoanalyse und Risikobewertung dann vornehmen, wenn ihre besondere Situation oder die Entwicklung der Risiken dies erfordern.</p> <p>Zu Absatz 2</p> <p>Die Festlegung methodischer und inhaltlicher Vorgaben durch das BBK folgt der umfangreichen fachlichen, sektorenübergreifenden und methodischen Expertise im Bereich des physischen Schutzes von Betreibern kritischer Anlagen. Hierfür können den Betreibern kritischer Anlagen insbesondere Vorlagen und Muster durch das BBK zur Verfügung gestellt werden.</p>	
	<p>Zu § 10 (Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan)</p> <p>Zu Absatz 1</p> <p>Im Einklang mit Artikel 13 der Richtlinie (EU) 2022/2557 werden Betreiber kritischer Anlagen dazu verpflichtet, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen. Diese Maßnahmen sind entsprechend Artikel 13 Abs. 1 der Richtlinie (EU) 2022/2557 auf der Grundlage der nach § 8 bereitgestellten Informationen über die nationalen Risikoanalysen und Risikobewertungen sowie den Ergebnissen der eigenen Risikoanalysen und Risikobewertung nach § 9 zu treffen. Mit dieser Regelung soll ein risikobasierter All-Gefahren-Ansatz beim Ergreifen von Maßnahmen zur Stärkung der Resilienz verfolgt werden.</p> <p>In den Nummern 1 – 6 werden die Ziele dargestellt, die mit den Maßnahmen erreicht werden sollen.</p> <p>Bei den von den Betreibern kritischer Anlagen zu treffenden technischen, sicherheitsbezogenen und organisatorischen Maßnahmen ist die Verhältnismäßigkeit zu wahren. Diese ist gewahrt, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls zum Risiko eines Vorfalles angemessen erscheint. Dabei können auch wirtschaftliche Aspekte berücksichtigt werden.</p> <p>Zu Absatz 2</p> <p>Die Resilienzmaßnahmen müssen auf den nationalen Risikoanalysen und Risikobewertungen gemäß § 8 sowie auf den Risikoanalysen und Risikobewertung der Betreiber kritischer Anlagen beruhen. Dabei soll der Stand der Technik eingehalten werden. Bei der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Ergreifen solcher Maßnahmen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.</p> <p>Zu Absatz 3</p> <p> Absatz 3 enthält eine beispielhafte Auflistung von Maßnahmen, die die Betreiber kritischer Anlagen bei der Abwägung, welche Maßnahmen zur Erreichung der Ziele nach Absatz 1 geeignet und verhältnismäßig sind, berücksichtigen können.</p> <p> Absatz 3 Nummer 5 b enthält eine Klarstellung, dass das von den Betreibern kritischer Anlagen zu berücksichtigende Sicherheitsmanagement im Hinblick auf Zuverlässigkeitsüberprüfungen hinsichtlich der Mitarbeitenden unbeschadet der Vorschriften des Sicherheitsüberprüfungsgesetzes (SUG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SUV) sowie unbeschadet weiterer Fachgesetze wie dem Atomgesetz, dem Luftverkehrsgesetz, dem Sicherheitsgewerbe-gesetz und der Hafensicherheitsgesetze erfolgt.</p> <p>Zu Absatz 4</p> <p>Auf Grund der Verschiedenheit der Sektoren, werden sich unterschiedliche Maßnahmen in Bezug auf ihre Geeignetheit und Verhältnismäßigkeit in den</p>	
	<p>Zu § 11 (Nachweise; behördliche Anordnungen)</p> <p>Zu Absatz 1</p> <p>Sofern die Einhaltung der Maßnahmen nach Absatz 1 kontrolliert werden soll, kann die für den Betreiber einer kritischen Anlage zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe vom Bundesamt für Sicherheit in der Informationstechnik die Übersendung derjenigen Bestandteile des Nachweises der Einhaltung der Maßnahmen nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen verlangen, die für die Überprüfung der Einhaltung der Maßnahmen nach § 10 Absatz 1 erforderlich sind. Dies dient der Reduzierung der Bürokratie und stellt eine Verbindung dazu her, dass bereits nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen Maßnahmen umfasst sind, die auch der physischen Resilienz von Betreibern kritischer Anlagen dienen und nach dem KRITIS-DatG verlangt werden.</p> <p>Zu Absatz 2</p> <p>Sofern die übermittelten Informationen zur Feststellung der Erfüllung der Verpflichtungen nach § 10 Absatz 1 nicht ausreichen, kann die für den Betreiber einer kritischen Anlage zuständige Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder die zuständige Behörde der Länder nach § 3 Absatz 5 den Betreiber einer kritischen Anlage zur Vorlage weiterer Informationen und geeigneter Nachweise zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 auffordern.</p> <p>Zu Absatz 3</p> <p>Der Nachweis kann durch Audits erfolgen.</p> <p>Zu Absatz 4</p> <p>Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann zur Ausgestaltung des Verfahrens der Erbringung des Nachweises und der Audits Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber kritischer Anlagen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festlegen.</p> <p>Zu Absatz 5</p> <p> Absatz 5 dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2022/2557.</p> <p>Zu Absatz 6</p> <p> Absatz 6 dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2022/2557.</p>	<p>Zu Absatz 1: Warum müssen diese Informationen zu Risiken und Maßnahmen (Resilienzpläne) hin und her geschickt werden, reicht nicht die Bestätigung von einer Behörde an die nächste, dass die getroffenen Maßnahmen für den physischen Schutz ausreichen? Wenn dem nicht so ist, muss sicher gestellt werden, dass diese sensiblen Daten ausreichend geschützt werden.</p>

	<p>Zu § 12 (Meldewesen für Vorfälle)</p> <p>Zu Absatz 1</p> <p>Im Einklang mit der Begründung zur Richtlinie (EU) 2022/2557 soll dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe mit der Einrichtung eines zentralen Meldewesens für die Meldung bestimmter Vorfälle ermöglicht werden, sich einen umfassenden Überblick über die Auswirkungen, die Art, die Ursache und die möglichen Folgen von Störungen und die Abhängigkeiten der Sektoren zu verschaffen.</p> <p>Betreiber kritischer Anlagen sind verpflichtet, den zuständigen Behörden unverzüglich Vorfälle zu melden, die die Erbringung kritischer Dienstleistungen erheblich stören oder erheblich stören könnten.</p> <p>Die Meldung erfolgt an eine mit dem Bundesamt für Sicherheit in der Informationstechnik eingerichtete gemeinsame Meldestelle. Bereits jetzt sind Betreiber kritischer Infrastrukturen (derzeitige Begriff nach § 2 Absatz 10 BSIg) verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik über ein Online-Meldeportal gemäß § 8b Abs. 4 Nr. 1 BSIg Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben, zu melden.</p> <p>Nach § 8 Abs. 4 Nr. 2 BSIg sind Betreiber kritischer Infrastrukturen ferner verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik über ein Online-Meldeportal auch erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen könne, zu melden.</p> <p>Das bereits existierende Online-Meldeportal des Bundesamtes für Sicherheit in der Informationstechnik wird für Störungen nach diesem Gesetz, die den physischen Schutz von Be-treibern kritischer Anlagen betreffen, erweitert. Hierdurch wird der Verwaltungsaufwand sowohl für die beteiligten Behörden aber auch der Betreiber erheblich reduziert.</p> <p>Die Störungsmeldung nach diesem Gesetz erfolgt unbeschadet anderer gesetzlicher Meldeverpflichtungen gegenüber weiteren zuständigen Behörden. Bereits bestehende Mel-dungsverpflichtungen der Betreiber gegenüber anderen Stellen, bleiben daher, sofern ge-geben, bestehen.</p> <p>Zu Absatz 2</p> <p>Absatz 2 setzt Art. 15 Abs. 2 S. 1 i.V.m. Art. 15 Abs. 1 S. 1 a) – c) der Richtlinie (EU) 2022/2557 um.</p> <p>Zu Absatz 3</p> <p>Betreiber kritischer Anlagen übermitteln spätestens 24 Stunden nach Kenntnis von einem Vorfall eine erste Meldung. Der Umfang der Erstmeldung sollte lediglich diejenigen Informa-tionen enthalten, die unbedingt erforderlich sind, um das BBK über den Vorfall zu unterrich-ten. In einer solchen Meldung sollte, soweit möglich, die mutmaßliche Ursache des Vorfalles angegeben werden. Betreiber kritischer Anlagen haben sicherzustellen, dass die Ressour-cen zur</p>	<p>Zu Absatz 1: Warum können sich weitere Behörden nicht auch dieses Meldeportals bedienen, und die Betreiber somit nur eine Meldung absetzen?</p> <p>Zu Absatz 3: Was macht das BBK mit diesen Meldungen? Zeitversetzte Lageberichte erscheinen uns nicht so wichtig wie zeitnahe Warnung an andere Betreiber, damit diese sich bei Bedarf schützen können. Diese Absicht finden wir nicht in der jetzigen Version des KRITIS Dachgesetzes. Das BSI lebt das auch schon mit den "Tageslageberichten" und "Ad-Hoc-Lageberichten" vor.</p>
	<p>Zu § 13 (Unterstützung der Betreiber kritischer Anlagen)</p> <p>Zu Absatz 1</p> <p>Absatz 1 dient der Umsetzung von Artikel 10 Absatz 1 Satz 1 und Satz 2 der Richtlinie (EU) 2022/2557. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe verfügt bereits heute über Expertise beim Schutz kritischer Infrastrukturen und hat Leitfäden erarbeitet und bietet Schulungen für Betreiber kritischer Infrastrukturen an. Durch die im KRITIS-Dachgesetz hinzukommenden Aufgaben wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eine noch größere Fachexpertise entwickeln, die insbesondere sekt-rübergreifende und die Interdependenzen betrachtende Aspekte sowie Vorfälle bei Betrei-bern kritischer Anlagen umfasst. Dadurch kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die Betreiber kritischer Anlagen bei der Stärkung ihrer Resilienz und der Entwicklung von effektiven Resilienzmaßnahmen unterstützen. Das Bundesamt für Bevöl-kerungsschutz und Katastrophenhilfe soll dabei mit anderen Behörden und insbesondere den anderen zuständigen Behörden, den Aufsichtsbehörden des Bundes und den Landes-behörden zusammenarbeiten, um auf sektorspezifische Expertise zurückzugreifen</p> <p>Zu Absatz 2</p> <p>Absatz 2 dient der Umsetzung von Artikel 13 Absatz 4 der Richtlinie (EU) 2022/2557. Eine Beratungsmission dient der Unterstützung des Betreibers der kritischen Anlage, indem sie im Hinblick auf die Erfüllung ihrer Verpflichtungen nach §§ 9 bis 12 beraten wird. Die Ein-richtung einer solchen Beratungsmission setzt nach der Richtlinie (EU) 2022/2557 einen Antrag eines Mitgliedsstaats voraus. Auf nationaler Ebene wird diese Aufgabe vom Bundes-ministerium des Innern und für Heimat wahrgenommen. Die betreffende Einrichtung muss der Beratungsmission zustimmen. Die Beratungsmission erstattet der Europäischen</p>	
	<p>Zu § 14 (Billigungs-, Überwachungs-, und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen)</p> <p>Zu Absatz 1</p> <p>Die Regelung des § 14 entspricht der Regelung nach [§ 38 des Gesetzes über das Bun-desamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informations-technik von Einrichtungen].</p> <p>Geschäftsleiter von Betreibern kritischer Anlagen trifft eine besondere Überwachungspflicht die Einhaltung der Maßnahmen nach § 10 Absatz 1 und ihre Umsetzung zu überwachen. Auch bei Einschaltung von Hilfspersonen bleibt das Leitungsorgan letztverantwortlich. Die Bedeutung dieser Pflicht wird durch eine Haftungsregelung unterstrichen. Einrichtungen des Sektors öffentliche Verwaltung sind nach § 5 Absatz 3 von den Pflichten nach § 14 ausge-nommen.</p> <p>Zu Absatz 2</p> <p>Im Einklang mit der Regelung des § 38 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen müssen Geschäftsleiter regelmäßig an Schulungen teilnehmen. Dies zuständige Aufsichts-behörde kann darüber Nachweis verlangen.</p>	
	<p>Zu § 15 (Berichtspflichten)</p> <p>Zu Absatz 1</p> <p>Zu Nummer 1</p> <p>Im Einklang mit Art. 5 Abs. 4 der Richtlinie (EU) 2022/2557 sollen innerhalb von drei Mona-ten nach Durchführung von staatlichen Risikoanalysen und Risikobewertungen entspre-chende Informationen über die ermittelten Arten von Risiken und die Ergebnisse dieser Ri-sikobewertungen, aufgeschlüsselt nach den im Anhang genannten Sektoren und Teilsjekto-ren an die Europäische Kommission übermittelt werden.</p> <p>Zu Nummer 2</p> <p>Im Einklang mit Art. 7 Absatz 2 a) der Richtlinie (EU) 2022/2557 sollen die kritischen Dienst-leistungen, die über die Liste wesentlichen Dienste gemäß der Delegierten Verordnung (EU) 2023/2450 hinausgehen, übermittelt werden. Ebenso soll die Zahl der ermittelten kriti-schen Anlagen für jeden in der Rechtsverordnung nach § 16 festgelegten Sektor sowie die Schwellenwerte, die zur Identifizierung der kritischen Anlagen in der Rechtsverordnung nach § 16 festgelegt werden, an die Europäische Kommission übermittelt werden und min-destens alle vier Jahre aktualisiert werden.</p> <p>Zu Absatz 2</p> <p>Im Einklang mit Artikel 9 der Richtlinie (EU) 2022/2557 sollen bis zum 17. Juli 2028 und danach alle zwei Jahre legt das Bundesministerium des Innern und für Heimat der Europäi-schen Kommission und der gemäß Artikel 19 der Richtlinie (EU) 2022/2557 genannten Gruppe für die Resilienz kritischer Einrichtungen einen zusammenfassenden Bericht über die bei ihnen eingegangenen Meldungen nach § 12, einschließlich der Zahl der Meldungen, der Art der gemeldeten Vorfälle und der gemäß § 15 ergriffenen Maßnahmen, vor.</p> <p>Zu Absatz 3</p> <p>Die Begriffsbestimmung dient der Umsetzung von Artikel 1 Absatz 8 der Richtlinie (EU) 2022/2557.</p> <p>Zu Absatz 4</p> <p>Absatz 4 dient als Rechtsgrundlage für das Bundesamt für Bevölkerungsschutz, die erfor-derlichen Informationen, zur dessen Übermittlung sie der Europäischen Kommission über das Bundesministerium des Innern und für Heimat verpflichtet sind, um die notwendigen Informationen von den Aufsichtsbehörden in § 3 zu erhalten.</p> <p>Zu Absatz 5</p> <p>Siehe Begründung zu § 7 Absatz 5.</p> <p>Zu Absatz 6</p> <p>Die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die zuständigen Behörden der Länder nach § 3 Absatz 5 übermitteln dem Bundesamt für Bevölkerungs-schutz und Katastrophenhilfe jährlich einen zusammenfassenden Bericht über die Auf-sichtsmaßnahmen nach § 11. Dies muss zum ersten Mal bis</p>	
	<p>Zu § 16 (Ermächtigung zum Erlass von Rechtsverordnungen)</p> <p>Zu Absatz 1</p> <p>Die genannten Regelungen des Gesetzes bedürfen zwingend der näheren Ausgestaltung. Das Bundesministerium des Innern und für Heimat erhält daher die Ermächtigungsgrundla-ge zum diesbezüglichen Erlass von Verordnungen, die die Grundlage für den sachgerech-ten Vollzug der Regelungen beinhalten.</p> <p>In Absatz 1 werden die genannten Bundesministerien ermächtigt, die Rechtsverordnung zur Identifizierung von Betreibern kritischer Anlagen zu erlassen. Die Kritikalität einer Anlage wird zum einen durch die Zugehörigkeit zu einem Sektor und durch die Erbringung einer kritischen Dienstleistung definiert. Zum anderen wird sich an einem zentralen Regelschwellenwert orientiert.</p> <p>Der hier genannte Regelschwellenwert von 500.000 zu versorgenden Einwohnern stellt eine Grundlage für die Ermittlung angemessener und geeigneter branchenspezifischer Schwellenwerte dar, Abweichungen von diesem Regelschwellenwert können dabei im Ein-zelfall sinnvoll sein. Für die Bestimmung kritischer Anlagen können insbesondere neben einem rein statischen Regelschwellenwert von 500.000 zu versorgenden Einwohnern auch weitere quantitative und qualitative Kriterien mit einbezogen werden. Insbesondere können auch unter Zuhilfenahme qualitativer Kriterien (Beispiel: einzige versorgungsrelevante An-lage in einem größeren Umkreis oder aufgrund ihrer technischen Eigenschaften besonders relevante Anlage) bei einzelnen Anlagenkategorien mehrere unterschiedliche quantitative Kriterien festgelegt werden, um eine möglichst sachgerechte Bestimmung kritischer Anla-gen sicherzustellen. Hierbei ist grundsätzlich ein ähnliches Verfahren wie in der derzeitigen Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) geplant, auch hier werden beispielsweise für Stromerzeugungsanlagen mehrere unterschiedliche quantitative Schwellenwerte definiert. Hierdurch werden bei-spielsweise für die Versorgungssicherheit besonders relevante schwarzstarzfähige Erzeu-gungsanlagen oder Erzeugungsanlagen, die Primärregelleistung erbringen, mit eigenen, niedrigeren Schwellenwerten berücksichtigt.</p> <p>Darüber hinaus können für weitere besonders bedeutsame und gegebenenfalls besonders gefährdete Einrichtungen wie z.B. Flughäfen, der Regelschwellenwert, die Bemessenskrite-rien oder die sektorspezifischen Schwellenwerte angepasst werden.</p> <p>Zu Absatz 2</p> <p>Die Rechtsverordnungsmächtigung schafft die Möglichkeit, sektorspezifische Regelungen durch die für den Sektor zuständigen Bundesministerien zu erlassen <u>wie in § 10 Absatz 5 vorgesehen</u>.</p>	

	<p>Zu § 17 (Ausnahmebescheid)</p> <p>§ 17 dient der Umsetzung von Artikel 1 Absatz 6-bis 8 der Richtlinie (EU) 2022/2557. Damit wird von der Möglichkeit der Schaffung einer Ausnahme für die Anwendung des KRITIS-DachG Gebrauch gemacht. Der Grund einer teilweisen oder vollständigen Ausnahme von den in Artikel 12, 13 und 15 der Richtlinie (EU) 2022/2557 – umgesetzt in den § 6 ff. – genannten Pflichten ist die Wahrung des nationalen Sicherheitsinteresses. So ist es in den Erwägungsgründen 11 der Richtlinie (EU) 2022/2557 angelegt, dass es zur Wahrung wesentlicher Interessen der nationalen Sicherheit, dem Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit der Mitgliedstaaten erforderlich sein muss, Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung von obigen Pflichten auszunehmen, wenn derartige Auskünfte oder eine Preisgabe dem nationalen Sicherheitsinteresse zuwiderliefe. Als relevante Bereiche führt Artikel 1 Absatz 6 und 7 der Richtlinie (EU) 2022/2557 die Bereiche der nationalen Sicherheit, öffentlichen Sicherheit, der Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten an. Um dem Sinne einer Ausnahmeregelung, die nicht zu weit greift, gerecht zu werden, ist ein Ausgleich zwischen einem „hohen Resilienzniveau“ (siehe Erwägungsgrund 8 der Richtlinie (EU) 2022/2557) und dem Mitgliedstaatsinteresse der Wahrung nationaler Sicherheitsinteressen zu erbringen.</p> <p>Bei dem hiesigen Befreiungsbescheid ist von einem nichtbegünstigenden Verwaltungsakt auszugehen. Gemäß § 48 Absatz 1 Satz 2 VwVfG bestimmt die Legaldefinition die Begünstigung wie folgt: Ein Verwaltungsakt ist begünstigend, wenn er ein Recht oder einen rechtlich erheblichen Vorteil begründet oder bestätigt. Ein Recht könnte in der Art begründet sein, als dass die der Befreiung unterliegende Betreiber der kritischen Anlage oder der Einrichtung der Bundesverwaltung entweder ganz oder teilweise den Pflichten der § 8 ff. nicht nachkommen muss. Andererseits entfallen diese Pflichten nicht einfach. Eine Begünstigung ist nach dem objektiven Regelungsgehalt des Verwaltungsakts unter Berücksichtigung des Zwecks der ihm zugrunde liegenden Norm zu beurteilen, nämlich derart, dass eine Befreiung von obigen Pflichten nicht dem Betreiber der kritischen Anlage oder der Einrichtung der Bundesverwaltung, die den Ausnahmebescheid erhält, sondern dem nationalen Sicherheitsinteresse zugutekommen. Der Ausnahmebescheid soll gerade kein Recht verleihen, sondern nur die Pflichten des Adressaten des Ausnahmebescheids anderweitig ausgestalten, zumal gleichwertige Maßnahmen, die denen der Befreiung gleichkommen nach Sinn und Zweck getroffen werden müssen.</p> <p>Zu Absatz 1</p> <p>Zunächst wird obig genanntes Ziel durch ein begrenztes Vorschlagsrecht, durch Bundeskanzleramt, Bundesministerium für Verteidigung, Bundesministerium des Innern und für Heimat, Bundesministerium der Justiz und der Ministerien für Inneres und Justiz der Länder entsprochen. Dabei ist ein Antragsrecht der betreffenden Einrichtung bewusst nicht vorgesehen. Weiterhin einschränkend wirken die umfassten Bereiche der Betreiber kritischer Anlagen und der Einrichtungen der Bundesverwaltung. Hierbei wird insbesondere auf die auch in der CER-Richtlinie explizit genannten, rechtlich anerkannten Kategorien, der öffentlichen Sicherheit und Ordnung verwiesen. Als Begrenzung der Ausnahmeregelung einzubeziehender Erwägungsgrund sollte auf die Wesentlichkeit der Interessen der nationalen Sicherheit abzustellen sein.</p>	
	<p>Zu § 18 (Verarbeitung personenbezogener Daten)</p> <p>Zu Absatz 1</p> <p>Mit § 18 wird auf der Grundlage von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e der Verordnung (EU) 2016/679 eine bereichsspezifische Rechtsgrundlage zur Verarbeitung personenbezogener Daten geschaffen</p> <p>Zu Absatz 2</p> <p>Absatz 2 ermöglicht die Weiterverarbeitung personenbezogener Daten. Die Regelung trägt dem Erfordernis Rechnung, dass das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie die anderen mit dem Vollzug des Gesetzes beauftragten zuständigen Aufsichtsbehörden des Bundes oder des Landes nach § 3 Absatz 3 und Absatz 5 sowie das Bundesamt für Sicherheit in der Informationstechnik, die Bundesnetzagentur, die Bundesanstalt für Finanzdienstleistungsaufsicht für die Erfüllung ihrer gesetzlichen Aufgaben eine datenschutzrechtliche Rechtsgrundlage benötigen, um personenbezogene Daten zum Zwecke der Sammlung, Auswertung und Untersuchung von Vorfällen nach § 12 dieses Gesetzes und zur Unterstützung, Beratung und Warnung in Fragen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen zu verarbeiten. Die in Absatz 1 genannten Behörden müssen in der Lage sein, zur Erfüllung ihrer Aufgaben aus § 3 alle ihnen aus öffentlichen, privaten, staatlichen, bekannten oder anonymen Quellen erlangten und zur Verfügung gestellten Daten auszuwerten, um Betreiber kritischer Anlagen dabei zu unterstützen, angemessene Resilienzmaßnahmen über die bereits bestehenden hinaus zu entwerfen oder zu etablieren. Hierzu ist allerdings auch eine Interessenabwägung erforderlich.</p> <p>Zu Absatz 3</p> <p>Absatz 3 verweist auf § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes. Den in Absatz 1 genannten Behörden steht es frei, zur Wahrung der Interessen der betroffenen Person darüber hinaus weitere geeignete technische oder organisatorische Maßnahmen zu ergreifen.</p>	
	<p>Zu § 19 (Bußgeldvorschriften)</p> <p>Hinweis: Die Begründung ist noch nicht vollständig den Änderungen des § 19 angepasst worden.</p> <p>§ 19 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2022/2557. Danach müssen die Mitgliedstaaten bei Verstößen gegen die in diesem Gesetz umgesetzten Vorgaben aus der Richtlinie (EU) 2022/2557 Sanktionen erlassen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.</p> <p>Zu Absatz 1</p> <p>Zu Absatz 2</p> <p>[...]</p> <p>Zu Absatz 3</p> <p>[...]</p>	Der UP KRITIS empfiehlt, erst nach der ersten Evaluierung des KRITIS Dachgesetzes Unternehmen mit Bußgeldern bei Nichterfüllung zu sanktionieren (siehe Anmerkung zu §19).
	<p>Zu § 20 (Evaluierung)</p> <p>Gemäß dem Beschluss des Staatssekretärausschusses Bessere Rechtsetzung und Bürokratieabbau vom 23. Januar 2013 sind wesentliche Regelungsvorhaben zu evaluieren. Das KRITIS-DachG ist als ein solches wesentliches Regelungsvorhaben anzusehen. Mit dem Ziel, erstmalig sektorenübergreifende physische Resilienzmaßnahmen für Betreiber kritischer Anlagen vorzusehen und damit die Aufrechterhaltung der Wirtschaftsstabilität angesichts der wechselseitigen Abhängigkeiten zu regeln, werden Regelungsinhalte getroffen, deren Auswirkungen sowohl für die Wirtschaft als auch für den Verwaltungsvollzug noch nicht vollständig bekannt sind und zum aktuellen Zeitpunkt auch noch nicht vollständig abgeschätzt werden können. Durch erste Abschätzungen der Erfüllungsaufwände besteht eine große Wahrscheinlichkeit, dass die jährlichen Erfüllungsaufwände für Wirtschaft und Verwaltung jeweils 1 Mio. EURO überschreiten.</p> <p>Mit der Evaluierungsklausel soll ein kontinuierlich wirkendes qualitatives Überprüfungs-instrument etabliert werden, ob die Zielsetzung des KRITIS-DachG, der Aufrechterhaltung der Wirtschaftsstabilität angesichts der wechselseitigen Abhängigkeiten, erreicht wird. Evaluiert werden soll insbesondere, ob</p> <ul style="list-style-type: none"> -Betreiber kritischer Anlagen nach den Bestimmungen dieses Gesetzes angemessen, bürokratiearm und zielorientiert identifiziert werden können, -die Identifizierung von Betreibern kritischer Anlagen erweitert werden sollte, -das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die weiteren zuständigen Behörden, Aufsichtsbehörden des Bundes und die zuständigen Behörden der Länder ihren Aufgaben aus diesem Gesetz hinreichend nachkommen können, insbesondere in fachlich sachkundiger und personeller Hinsicht, aber auch hinsichtlich der erforderlichen Ausstattung, -die Zusammenarbeit und der Informationsaustausch zwischen dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, den weiteren zuständigen Behörden, den Aufsichtsbehörden des Bundes und den zuständigen Behörden der Länder funktioniert, -sich stichprobenartigen Kontrollen nach § 11 bewährt haben, -Widersprüche bei Regelungen der Länder in Umsetzung des KRITIS-Dachgesetzes bestehen und ob der Bund von der Konkurrenz der konkurrierenden Gesetzgebungskompetenz (Recht der Wirtschaft) Gebrauch macht, um Bundes einheitlichkeit herzustellen <p>Die Bundesregierung legt frühestens nach Ablauf von 5 Jahren, spätestens nach Ablauf von 7 Jahren nach Inkrafttreten des Gesetzes einen Evaluierungsbericht vor. Aus diesem sollte insbesondere hervorgehen,</p> <ul style="list-style-type: none"> -ob das Ziel des Gesetzes erreicht wurde, -welche Kosten und Nutzen bei der Umsetzung dieses Gesetzes entstanden sind, -ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist und -welche weiteren Schlussfolgerungen oder Handlungsoptionen oder Vorgehensweisen empfohlen werden (Handlungsempfehlungen) <p>Gemäß Art. 25 der Richtlinie (EU) 2022/2557 nimmt die Europäische Kommission eine eigene Evaluierung der Richtlinie (EU) 2022/2557 vor. Sie legt den ersten</p>	
	<p>Zu Artikel 2 (Änderung des Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG))</p> <p>Zu Nummer 1</p> <p>Die für kritischen Dienstleistungen jeweils zuständigen Landesregierungen können zeitlich gestaffelt Rechtsverordnungen zur sektorspezifischen Konkretisierung von Resilienzmaßnahmen erlassen. Artikel 2 ändert § 10 des KRITIS-Dachgesetzes durch Ergänzung einer Ermächtigung der Landesregierungen für Rechtsverordnungen zur Festlegung sektorspezifischer Mindestvorgaben für Resilienzmaßnahmen, solange und soweit kein entsprechender branchenspezifischer Resilienztandard gemäß § 10 Absatz 6 Satz 2 durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe als geeignet anerkannt wurde. Der Entwicklung und Anerkennung von branchenspezifischen Resilienztstandards und damit bundesweit einheitlicher Resilienztstandards soll der Vorrang gegeben werden vor einer Verordnungsermächtigung für die Landesregierungen.</p> <p>Zu Nummer 2</p> <p>Durch die in Nr. 1 bedingte Einschubung des Absatzes 7 wird der in Art. 1 Absatz 7 zu Absatz 8.</p> <p>Zu Nummer 3</p> <p>Durch die in Nr. 1 bedingte Einschubung des Absatzes 7 wird der in Art. 1, § 10 Absatz 8 zu Absatz 9</p> <p>Zu Nummer 4</p> <p>Durch die in Nr. 1 bedingte Einschubung des Absatzes 7 wird der in dem Art. 1, § 10 Absatz 9 zu Absatz 10</p> <p>Zu Nummer 5</p> <p>Durch die in Nr. 1 bedingte Einschubung des Absatzes 7 wird der in Art. 1, § 10 Absatz 10 zu Absatz 11</p>	
	<p>Zu Artikel 3 (Inkrafttreten)</p> <p>Zu Absatz 1</p> <p>Das Gesetz in Artikel 1 tritt mit Ausnahme der Absätze 2 und 3 am Tag nach der Verkündung in Kraft.</p> <p>Zu Absatz 2</p> <p>Die §§ 6 bis 8, §§ 10 bis 12 und § 16 in Artikel 1 treten abweichend von Absatz 1 am 17. Juli 2026 in Kraft. Damit wird eine ausreichende Übergangszeit zwischen dem Inkrafttreten der gesetzlichen Bestimmungen und der Anwendung der den Betreibern kritischer Anlagen auferlegten Verpflichtungen vorgesehen, damit sie sich auf die Verpflichtungen nach diesem Gesetz einstellen und die erforderlichen Vorbereitungen treffen können. Die Frist ermöglicht gleichzeitig die Einhaltung der Anforderung des Artikels 6 Absatz 1 Richtlinie (EU) 2022/2557, nach der die Betreiber kritischer Anlagen bis zum 17. Juli 2026 ermittelt werden müssen.</p> <p>Zu Absatz 3</p> <p>Die in § 19 Absatz 1 Nummer 3 bis 11 in Artikel 1 vorgesehenen Bußgeldvorschriften treten abweichend von Absatz 1 erst am Werktag auf den folgenden Tag in Kraft, nachdem das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe branchenspezifische Resilienztstandards nach § 10 Absatz 6 als geeignet zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 festgestellt hat, frühestens jedoch am 17. Juli 2026</p> <p>Zu Absatz 4</p> <p>Die Änderung in Artikel 2 tritt am 01. Januar 2029 in Kraft.</p>	