COT Legal
Rechtsanwältin Claudia Otto

COT Legal
Rechtsanwältin Claudia Otto, MBA
Rudolf-Diesel-Str. 11
69115 Heidelberg
E-Mail: claudia.otto@cotlegal.de
Key: https://keys.openpgp.org
Internet: https://cotlegal.de
Threema/Fon: PJ726PHA

Leitfaden

Der Resilienzplan nach dem KRITISDachG:

Grundlagen, Methodik & Anforderungen

3. August 2026

TL;DR (Abschnitte A. und B.): Grundlagen von Resilienzplanung und -plan

Problem	Wo?	Lösung
Resilienz als Fähigkeit einer Anlage?	§ 2 Nr. 5 KRITISDachG	Resilienz ist die (Handlungs-)Fähigkeit des Betreibers einer kritischen Anlage.
Risikodefinition und Risikoformel sind ungenügend und nicht anwendergerecht.	§ 2 Nr. 6 KRITISDachG	Risikodefinition und Risikoformel sind durch Auslegung für Staat und Betreiber anzupassen.
Das Erfordernis der „Geeignetheit" von Resilienzmaßnahmen wurde gestrichen.	§ 13 Abs. 2 S. 1 KRITISDachG	Die „Geeignetheit" ist wegen der Resilienzzielbindung ungeschriebenes Merkmal.
Flucht in Wirtschaftlichkeitserwägungen?	§ 13 Abs. 2 S. 4 und 5 KRITISDachG	Das KRITISDachG lässt die Wirtschaftlichkeitsklauseln leerlaufen.
Keine Nennung von Gefahr, Bedrohung, Vulnerabilität.	KRITISDachG	KRITISDachG führt Gefahren & Bedrohungen als „Risiken". „Schwachstelle" meint „Vulnerabilität".
Ein Vorfall ist immer eine Gefahr, nie ein Risiko. Er kommt zudem selten allein.	§ 2 Nr. 9 KRITISDachG	Wortlaut, thematisierte Interdependenzen und Kaskadeneffekte legen dies nahe.

TL;DR (Abschnitt C.): Anforderungen an den Resilienzplan

Anforderungen	Wonach?	Umsetzung
Formale Anforderungen		
Risk-Assessment-Bezug	§ 13 Abs. 4 iVm Abs. 1-3 KRITIS-DachG; Art. 13 Abs. 1 CER-RL	Risk Assessment in wesentlichen Zügen darstellen und Maßnahmen-auswahl im Plan begründen.
Prüf- & Anpassungsfähigkeit	§ 16 Abs. 2 S. 2, Abs. 5 iVm Abs. 2 S. 2 KRITISDachG	Für Behördenprüfung nachvollziehbar gestalten und in modifizierbarer Form vorhalten.
Bezeichnung & Formfreiheit	§ 13 Abs. 4 und 5 KRITISDachG vs. Art. 13 Abs. 2 S. 1, 2 CER-RL	„Resilienzplan" (KRITISDachG) vs. Formfreiheit (CER-RL): Abweichende Dokumentation nur nach Behördenrücksprache.
Inhaltliche Anforderungen (Resilienzplan-Algorithmus)		
(Neu-)Konzeption für X	PDCA-Zyklus (Plan)	1. Rollen & Ressourcen 2. Prozesse & Schnittstellen 3. Vorgaben & Ziele.
Operationalisierung für X	PDCA-Zyklus (Do)	1. Selektion & Priorisierung 2. Umsetzung & Dokumentation 3. Information & Kommunikation
Evaluierung für X	PDCA-Zyklus (Check)	1. Messung & Abgleich 2. Unabhängigkeit & Qualität 3. Reporting & Transparenz.
Anpassung für X	PDCA-Zyklus (Act)	1. Auslöseereignisse & Eskalation 2. Evolution & Nachbereitung 3. Korrektur & Nachverfolgung.

A. Grundlagen der Resilienzplanung

Resilienzplanung einschließlich Resilienzplanerstellung erfordert Resilienzverständnis:

I. Was ist Resilienz im Sinne von CER-Richtlinie bzw. KRITIS-Dachgesetz?

Nach Art. 2 Nr. 2 der Richtlinie (EU) 2022/2557 vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen („Critical Entities Resilience", kurz: CER-Richtlinie oder CER-RL) meint „Resilienz" die Fähigkeit einer kritischen Einrichtung,

1. einen Sicherheitsvorfall zu verhindern,
2. sich davor zu schützen,
3. darauf zu reagieren,
4. einen solchen abzuwehren,
5. die Folgen eines solchen Vorfalls zu begrenzen,
6. einen Sicherheitsvorfall aufzufangen,
7. zu bewältigen und
8. sich von einem solchen Vorfall zu erholen.

Nach § 2 Nr. 5 des deutschen Gesetzes zur Umsetzung der CER-Richtlinie, dem KRITIS-Dachgesetz (KRITISDachG), meint „Resilienz" die Fähigkeit einer kritischen Anlage,

1. einen Vorfall zu verhindern,
2. sich vor einem Vorfall zu schützen,
3. einen Vorfall abzuwehren,
4. auf einen Vorfall zu reagieren,
5. die Folgen eines Vorfalls zu begrenzen,
6. einen Vorfall aufzufangen und
7. zu bewältigen und
8. sich von einem Vorfall zu erholen.

Beide Definitionen weichen ausweislich ihres Wortlauts voneinander ab. Die Abweichung wirkt sich bei näherer Betrachtung und sachgerechter Rechtsanwendung jedoch nicht aus:

1. Was ist eine kritische Einrichtung bzw. kritische Anlage?

Eine „kritische Einrichtung" meint nach der CER-Richtlinie eine öffentliche oder private Einrichtung, die ein Mitgliedstaat einer der Kategorien in der dritten Spalte der Tabelle im Anhang zugeordnet hat (Art. 2 Nr. 1 CER-RL). Anschaulicher beschreibt z.B. Erwägungsgrund 1 der CER-Richtlinie kritische Einrichtungen als *Anbieter* wesentlicher Dienste, denen eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt zukommt. Erwägungsgrund 3 der CER-Richtlinie spricht von Einrichtungen, die kritische Infrastrukturen *betreiben* und besser ausgestattet werden sollen, um auf Risiken für ihren Betrieb *reagieren* zu können, die zur Störung der Erbringung von wesentlichen Diensten führen könnten. Der Anhang spricht von Unternehmen, Betreibern, Erzeugern und Marktteilnehmern. Eine „kritische Einrichtung" im Sinne der CER-Richtlinie meint also eine Organisation als Trägerin von Rechten und Pflichten mitsamt ihren nicht-physischen und physischen Gegebenheiten (z.B. Fähigkeiten und örtlichen Bedingungen).

„Kritische Infrastrukturen" meint nach der CER-Richtlinie Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind (Art. 2 Nr. 4 CER-RL). Sie werden also von kritischen Einrichtungen *betrieben*.

Eine „kritische Anlage" im Sinne des KRITIS-Dachgesetzes ist eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist (§ 2 Nr. 3 KRITISDachG). Eine „Anlage" im Sinne des KRITIS-Dachgesetzes ist eine Betriebsstätte, sonstige ortsfeste Installation, Maschine, Gerät, sonstige ortsveränderliche technische Installation oder Software und IT-Dienste, soweit sie nicht ausschließlich den Vorgaben des BSI-Gesetzes unterfallen (vgl. § 2 Nr. 2 KRITISDachG). Eine kritische Anlage meint erkennbar *keine* Organisation.

Das KRITIS-Dachgesetz definiert daher den „Betreiber kritischer Anlagen" als 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 oder mehrere kritische Anlagen ausübt (vgl. § 2 Nr. 1 KRITISDachG).

2. Was ist ein Sicherheitsvorfall bzw. Vorfall?

Ein „Sicherheitsvorfall" meint nach der CER-Richtlinie ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der nationalen Systeme zur Wahrung der Rechtsstaatlichkeit (Art. 2 Nr. 3 CER-RL).

Ein „Vorfall" im Sinne des KRITIS-Dachgesetzes ist ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte und nicht ausdrücklich ausgenommen ist (vgl. § 2 Nr. 9 KRITISDachG).

3. Was sind relevante Dienste bzw. Dienstleistungen?

Ein „wesentlicher Dienst" meint nach der CER-Richtlinie einen Dienst, der für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung ist (Art. 2 Nr. 5 CER-RL). Er richtet sich erkennbar am Resilienzziel der CER-Richtlinie aus.

Eine „kritische Dienstleistung" im Sinne des KRITIS-Dachgesetzes ist eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde (§ 2 Nr. 4 KRITISDachG). Sie richtet sich an den Folgen fehlender Resilienz aus. „Dienstleistung" ist dabei nicht im engen, klassischen deutschen Wortsinne zu verstehen, sondern eher als eine Leistung im Rahmen einer wichtigen gesellschaftlichen Funktion bzw. wichtigen wirtschaftlichen Tätigkeit.

II. Was ist also Resilienz im Sinne des KRITIS-Dachgesetzes?

„Resilienz" im Sinne des § 2 Nr. 5 KRITISDachG und im vorstehend beschriebenen Spannungsfeld ist eine besondere Handlungsfähigkeit, welche die Fähigkeiten umfasst,

1. einen Vorfall zu verhindern,
2. sich vor einem Vorfall zu schützen,
3. einen Vorfall abzuwehren,
4. auf einen Vorfall zu reagieren,
5. die Folgen eines Vorfalls zu begrenzen,
6. einen Vorfall aufzufangen und
7. zu bewältigen und
8. sich von einem Vorfall zu erholen.

Da eine Anlage selbst naturgemäß nicht wie beschrieben handeln kann, kann sie auch nicht „resilient" sein. Diese Fähigkeiten sind erkennbar organisationsbezogen. § 2 Nr. 5 KRITISDachG ist entsprechend auszulegen.

B. Grundlagen eines Resilienzplans

Nach § 13 Abs. 4 iVm Abs. 1, 2 S. 1 KRITISDachG ist der sog. Resilienzplan auf Grundlage der nationalen Risikoanalysen und Risikobewertungen sowie der Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen zu fassen. Seine Grundlagen werden nachfolgend in den wesentlichen Zügen dargestellt.

I. Risikobegriff

„Risiko" meint nach der CER-Richtlinie das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird (Art. 2 Nr. 6 CER-RL).

„Risiko" ist nach dem KRITIS-Dachgesetz das Potenzial für Ausfälle oder Beeinträchtigungen, die durch einen Vorfall verursacht werden, das als eine Kombination des Ausmaßes eines Ausfalls oder einer Beeinträchtigung und der Wahrscheinlichkeit des Eintretens des Vorfalls zum Ausdruck gebracht wird (§ 2 Nr. 6 KRITISDachG).

1. Korrekturbedarf

a. Grund für den Korrekturbedarf

Das „Risiko" wird nach der „Risikoformel" der vorstehend wiedergegebenen Risikodefinitionen von CER-Richtlinie und KRITIS-Dachgesetz in die folgenden, ausdrücklich zu kombinierenden Faktoren zerlegt:

1. das Ausmaß von Verlust oder Störung bzw. Ausfall oder Beeinträchtigung (Verf.: *Schadensschwere*) und
2. die Wahrscheinlichkeit des Eintretens des (Sicherheits-)Vorfalls (Verf.: *Ereigniseintrittswahrscheinlichkeit*).

Wenn auch nicht für jedermann auf den ersten Blick erkennbar, ist diese „Risikoformel" fehlerhaft.

b. Fehlerhaftigkeit der Risikoformel

Um den Fehler zu verdeutlichen, sei die klassische Risikoformel aus der Versicherungsmathematik[1] herangezogen:

> Risiko ist die Kombination aus der Wahrscheinlichkeit des Eintritts eines Schadens und der Schwere dieses Schadens,

dargestellt in der folgenden Gleichung:

$$\text{Risiko}_{\text{Schaden}} = \text{Wahrscheinlichkeit}_{\text{Schaden}} \times \text{Schwere}_{\text{Schaden}}$$

Risiko wird so – wenn auch in Grenzen – quantitativ bestimm- und darstellbar. Ein auch quantitative Methodiken einschließendes Risk Assessment fördert oft eine bessere Nachvollziehbarkeit von Maßnahmenwahl und -wirkung im Rahmen der Risikobewältigung und (z.B. behördlichen) Prüfung.

Die o.g. Risikodefinitionen sprechen jedoch nicht von Schaden, sondern benennen jeweils zwei Schadensformen. Die Risikodefinition der CER-Richtlinie beispielsweise nennt den Verlust (als endgültigen oder vollständigen Fortfall der Bereitstellung eines wesentlichen Dienstes[2]) und die Störung (als temporären Fortfall im Sinne einer quantitativen Beeinträchtigung und/oder als qualitative Beeinträchtigung der Bereitstellung eines wesentlichen Dienstes[3]).

Einen solchen kontextspezifischen Schaden zu bestimmen, ist unproblematisch. Die Risikodefinition und -formel der CER-Richtlinie verknüpft allerdings – ähnlich wie die des

---

[1] *Siedschlag/Stangl*, Katastrophenmanagement, tredition (2020), S. 20.
[2] Vgl. die deutsche und englische Sprachfassung des Art. 2 Nr. 7 CER-RL: „Verluste oder Störungen *bei* der Erbringung eines wesentlichen Dienstes" entspricht nicht dem englischen Original „loss or disruption *of* the provision of an essential service". Die Formulierung „bei der Erbringung" verengt den Anwendungsbereich unsachgemäß temporal und aktionsbezogen (im Sinne von „während der aktiven Leistungserbringung"). Das englische Original zielt hingegen auf den Verlust oder die Störung der Bereitstellung als solche ab. Dass der verengende Wortlaut der Intention hinter der Richtlinie widerspricht, belegt Erwägungsgrund 3 CER-RL: Dieser beklagt ausdrücklich bestehende Lücken sowie das Ungenügen bisheriger Schutzmaßnahmen und fordert, dass *„noch mehr unternommen werden [sollte]"*, um kritische Infrastrukturen gegenüber dynamischen und kaskadierenden Bedrohungen abzusichern.
[3] Wie vor.

KRITIS-Dachgesetzes – den Verlust(schaden) mit der Eintrittswahrscheinlichkeit des Ereignisses, dem Sicherheitsvorfall:

$$\text{Risiko}_{\text{Verlust(schaden)}} = \text{Wahrscheinlichkeit}_{\text{Sicherheitsvorfall}} \times \text{Schwere}_{\text{Verlust(schaden)}}$$

Ein Risiko kann aufgrund dieser Risikoformel nicht ermittelt werden. Sie setzt die Eintrittswahrscheinlichkeit des Ereignisses als Auslöser mit der Eintrittswahrscheinlichkeit des Schadens als Folge gleich. Das impliziert, dass ein Ereignis *immer* zu einem Schaden führt. Eine solche deterministische Beziehung zwischen Ereignis und Schaden gibt es jedoch nicht. Die o.g. Definitionen von Sicherheitsvorfall bzw. Vorfall zeigen nicht zuletzt, dass weder CER-Richtlinie noch KRITIS-Dachgesetz diese deterministische Beziehung als wahr unterstellen.

Hier liegt schlicht ein Fehler im Transfer der Inhalte verschiedener Definitionen vor, der durch Auslegung korrigiert werden kann.

c. Korrigierende Auslegung

Bei der korrigierenden Auslegung muss zum einen zwischen dem Risikobegriff für die nationale Risikobewertung durch den EU-Mitgliedstaat (hier: Deutschland nach Art. 5 CER-RL bzw. § 11 KRITISDachG) und dem Risikobegriff für die Risikobewertung durch die kritischen Einrichtungen selbst (nach Art. 12 CER-RL bzw. § 12 KRITISDachG) unterschieden werden.

Für die sachgerechte Risikoformelbildung und -behandlung ergeben sich zum anderen weitere Anhaltspunkte aus der CER-Richtlinie. So fällt beim Vergleich von CER-Richtlinie und KRITIS-Dachgesetz auf, dass die CER-Richtlinie in der deutschen Fassung nur „Risikobewertungen" verlangt, jedoch keine „Risikoanalysen". Das KRITIS-Dachgesetz zerlegt das Risk Assessment ausweislich der Definitionen in § 2 Nr. 7 und 8 KRITISDachG in Risikoanalyse und Risikobewertung. Hier verlangt der deutsche Gesetzgeber anscheinend mehr. Schaut man sich allerdings die Definition des Begriffs der „Risikobewertung" in Art. 2 Nr. 7 CER-RL sowie dessen englische Sprachfassung an, ist von „risk assessment" die Rede, welches als Gesamtprozess („overall process") die Risikoanalyse („analysing") und die anschließende Risikobewertung („evaluating") als Teilschritte umfasst. Das

KRITIS-Dachgesetz fordert hier also nicht mehr, es hat lediglich die letzten zwei Prozessschritte des Risk Assessments im Sinne der CER-Richtlinie normiert.

aa. Risikobegriff für Mitgliedstaaten

Mitgliedstaaten können kein Risk Assessment mit der vollen Tiefe und Detailliertheit durchführen, wie es die einzelnen kritischen Einrichtungen jeweils für sich tun müssten. Selbst im Falle einer Datenerhebung bei allen kritischen Einrichtungen wäre es ressourcenbedingt praktisch undenkbar, staatlicherseits ein Gesamt-Risk-Assessment anzubieten. Das Ergebnis würde nie im Bedarfszeitraum bereitstehen. Zugleich fehlt kritischen Einrichtungen regelmäßig das staatliche, ggf. geheimdienstliche Wissen in Bezug auf (geo-)politische sowie militärische Bedrohungen. Das staatliche Risk Assessment erfolgt daher aus einer Art Vogelperspektive, welche einen instruktiven Überblick über die Gefahren und Bedrohungen und ihre möglichen Auswirkungen für den jeweiligen Mitgliedstaat einschließlich seiner kritischen Einrichtungen geben soll. Der Abstraktionsgrad ist notwendigerweise hoch, um so viel Risk-Assessment-Bedarf wie nur möglich aufzuzeigen (Kompass-Funktion), zugleich aber noch genug notwendiges staatliches Wissen für die kritischen Einrichtungen bereitzustellen (Informations-Funktion).

Das National Risk Assessment 2023 des finnischen Innenministeriums[4] dient auch ohne formalen Bezug zur CER-Richtlinie als gutes Beispiel: Hier liegt der Fokus auf der relationalen Analyse und Einschätzung von typisierten Gefahren (hier v.a. „disruptions") und Bedrohungen („threats" bzw. „threat scenarios") sowie deren möglichen Auswirkungen („impact" oder „disruption impact"). „Risiko" meint hier das Ergebnis des „impact assessments", also der Kombination der funktionalen Bedeutung einer Säule staatlicher „Resilienz" („vital function") und dem Grad ihrer zu erwartenden Beeinträchtigung infolge der Auswirkung(en) („impact") von Gefahren und Bedrohungen. Die Erläuterungen zum Zwecke der Nachvollziehbarkeit und Zugrundelegung dieses „Risk Assessments" für weitere, konkretere Risk Assessments sind fachgerecht vorangestellt. Zudem werden die

[4] National Risk Assessment 2023 des finnischen Innenministeriums (Ministry of the Interior – Finland), abrufbar unter https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/072fa79a-f148-4fd2-af2d-38d925166a61/content (zuletzt abgerufen am 2. August 2026). Das Update ist für den Herbst 2026 angekündigt, vgl. Ministry of the Interior – Finland, National Risk Assessment, https://intermin.fi/en/rescue-services/preparedness/national-risk-assessment (zuletzt abgerufen am 2. August 2026).

Erwartungen sachgerecht auf das staatlicherseits Mögliche gelenkt und konkretere Risk Assessments verlangt.

Eine makroskopische „Risikobewertung" im Sinne eines Risk Assessments wie auch nach Vorgaben der CER-Richtlinie taugt dementsprechend nicht als Grundlage für die Risikobewältigung „am Boden" durch die einzelne kritische Einrichtung. Damit kann auch der Risikobegriff als Arbeitsgrundlage für die Mitgliedstaaten nicht derselbe Risikobegriff als Arbeitsgrundlage für die kritischen Einrichtungen sein.

Der Begriff „Risiko" kann für das staatliche Risk Assessment daher wie folgt verstanden werden:

> „Risiko" ist die Kombination der Wahrscheinlichkeit eines Verlusts oder einer Störung der Bereitstellung wesentlicher Dienste[5] infolge eines typisierten (Sicherheits-)Vorfalls und der Schwere der Auswirkungen dieses Verlusts oder dieser Störung.

bb. Risikobegriff für kritische Einrichtungen

Von kritischen Einrichtungen hingegen werden aufgrund ihrer Sach- und Wirknähe im Einzelfall konkrete, quasi mikroskopische Risk Assessments erwartet. Aufgrund des Vorstehenden bietet sich folgendes Verständnis des Begriffs „Risiko" für kritische Einrichtungen an:

> „Risiko" ist die Kombination der Wahrscheinlichkeit eines Verlusts oder einer Störung der Bereitstellung eines wesentlichen Dienstes[6] infolge eines konkreten (Sicherheits-)Vorfalls und der Schwere der Auswirkungen dieses Verlusts oder dieser Störung.

---

[5] Vgl. die deutsche und englische Sprachfassung des Art. 2 Nr. 7 CER-RL: „Verluste oder Störungen *bei* der Erbringung eines wesentlichen Dienstes" entspricht nicht dem englischen Original „loss or disruption *of* the provision of an essential service". Die Formulierung „bei der Erbringung" verengt den Anwendungsbereich unsachgemäß temporal und aktionsbezogen (im Sinne von „während der aktiven Leistungserbringung"). Das englische Original zielt hingegen auf den Verlust oder die Störung der Bereitstellung als solche ab. Dass der verengende Wortlaut der Intention hinter der Richtlinie widerspricht, belegt Erwägungsgrund 3 CER-RL: Dieser beklagt ausdrücklich bestehende Lücken sowie das Ungenügen bisheriger Schutzmaßnahmen und fordert, dass *„noch mehr unternommen werden [sollte]"*, um kritische Infrastrukturen gegenüber dynamischen und kaskadierenden Bedrohungen abzusichern.
[6] Wie vor.

Diese Auslegung lässt sich entsprechend auf § 2 Nr. 6 KRITISDachG übertragen.

2. Der mitgemeinte Verlust als Schadensvariante

Wie ausgeführt, spricht die Risikodefinition des Art. 2 Nr. 6 CER-RL nicht explizit von Schaden, sondern benennt zwei kontextspezifische Schadensformen: den „Verlust" als endgültigen oder vollständigen Fortfall der Bereitstellung eines wesentlichen Dienstes[7] und die „Störung" als temporären Fortfall im Sinne einer quantitativen Beeinträchtigung oder als eine qualitative Beeinträchtigung eines wesentlichen Dienstes.

§ 2 Nr. 6 KRITISDachG hingegen spricht von den kontextspezifischen Schadensformen „Ausfällen" und „Beeinträchtigungen". Das wirkt zunächst verengend.

Ausweislich Art. 12 Abs. 2 S. 1 CER-RL [8] sind es aber gerade die Extremfälle wie Naturereignisse oder Terroranschläge, deren irreversible Auswirkungen – also Verluste – vermieden werden sollen und die damit im Zentrum des Resilienzziels stehen:

> *Die Risikobewertung durch kritische Einrichtungen trägt allen entsprechenden natürlichen und vom Menschen verursachten Risiken Rechnung, die zu einem Sicherheitsvorfall führen könnten, einschließlich grenzüberschreitender oder sektorübergreifender Risiken, Unfällen, Naturkatastrophen, gesundheitlicher Notlagen und hybriden Bedrohungen und anderen feindlichen Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541.*[9]

---

[7] Vgl. die deutsche und englische Sprachfassung des Art. 2 Nr. 7 CER-RL: „Verluste oder Störungen *bei* der Erbringung eines wesentlichen Dienstes" entspricht nicht dem englischen Original „loss or disruption *of* the provision of an essential service". Die Formulierung „bei der Erbringung" verengt den Anwendungsbereich unsachgemäß temporal und aktionsbezogen (im Sinne von „während der aktiven Leistungserbringung"). Das englische Original zielt hingegen auf den Verlust oder die Störung der Bereitstellung als solche ab. Dass der verengende Wortlaut der Intention hinter der Richtlinie widerspricht, belegt Erwägungsgrund 3 CER-RL: Dieser beklagt ausdrücklich bestehende Lücken sowie das Ungenügen bisheriger Schutzmaßnahmen und fordert, dass *„noch mehr unternommen werden [sollte]"*, um kritische Infrastrukturen gegenüber dynamischen und kaskadierenden Bedrohungen abzusichern.

[8] Vgl. insbesondere Art. 5 Abs. 1 Unterabs. 2 CER-RL.

[9] Die Verwendung des Begriffs „Risiko" ist erkennbar auch in der CER-Richtlinie uneinheitlich und wird häufig mit dem Begriff der Gefahr verwechselt.

Da der Betreiber einer kritischen Anlage diese Extremfälle nach § 13 Abs. 2 S. 1 iVm § 11 Abs. 2 KRITISDachG zu berücksichtigen hat, kann § 2 Nr. 6 KRITISDachG so verstanden werden, dass der „Ausfall" den „Verlust" erfasst.

3. Geeignetheit als ungeschriebener Maßstab für Resilienzmaßnahmen

Nach Art. 13 Abs. 2 S. 1 CER-RL sind durch kritische Einrichtungen „geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz [zu] ergreifen". Der deutsche Gesetzgeber hat in § 13 Abs. 2 S. 1 KRITISDachG jedoch den Zusatz „geeignete" gestrichen.

Der Streichung liegt offenbar ein Missverständnis im Hinblick auf die Verhältnismäßigkeitsanforderung zugrunde. „Geeignetheit" meint hier nicht die Voraussetzung des öffentlich-rechtlichen Verhältnismäßigkeitsgrundsatzes[10] neben dem legitimen Zweck, der Erforderlichkeit und Angemessenheit staatlicher Maßnahmen mit Eingriffscharakter. Dieser gilt als „übergreifende Leitregel allen staatlichen Handelns"[11] nur dort, wo „sich Staat und Bürgerinnen und Bürger gegenübertreten"[12], um letztere vor staatlichen Grundrechtseingriffen zu schützen. § 13 KRITISDachG regelt jedoch das Resilienzmanagement einschließlich Maßnahmenbestimmung *aufgrund* des Risk Assessments (d.h. der „Risikobewertung" nach „Risikoanalyse", siehe oben) durch überwiegend privatrechtliche Akteure. Dass mancher Betreiber kritischer Anlagen öffentlich-rechtlich handeln darf, macht die Maßnahmen im Rahmen des Resilienzmanagements nicht zu einer staatlichen Maßnahme mit Grundrechtseingriffscharakter.

Der Gesetzgeber sollte den Zusatz der Geeignetheit in § 13 Abs. 2 S. 1 KRITISDachG daher aufnehmen. Da Maßnahmen nach § 13 Abs. 1 wegen Abs. 2 S. 1 KRITISDachG ausdrücklich „zur Erreichung der Ziele" zu treffen sind, ist die Geeignetheit bereits ungeschriebene

[10] Siehe dazu BMJV, Verhältnismäßigkeit als rechtsstaatliches Grundprinzip, 10. April 2023, abrufbar unter: https://www.bmjv.de/DE/rechtsstaat_kompakt/rechtsstaat_grundlagen/verhaeltnismaessigkeit/verhaeltnismaessigkeit_node.html (zuletzt abgerufen am 2. August 2026).
[11] BMJV unter Verweis auf BVerfGE 23, 127 (133), Verhältnismäßigkeit als rechtsstaatliches Grundprinzip, 10. April 2023, abrufbar unter: https://www.bmjv.de/DE/rechtsstaat_kompakt/rechtsstaat_grundlagen/verhaeltnismaessigkeit/verhaeltnismaessigkeit_node.html (zuletzt abgerufen am 2. August 2026).
[12] BMJV, Verhältnismäßigkeit als rechtsstaatliches Grundprinzip, 10. April 2023, abrufbar unter: https://www.bmjv.de/DE/rechtsstaat_kompakt/rechtsstaat_grundlagen/verhaeltnismaessigkeit/verhaeltnismaessigkeit_node.html (zuletzt abgerufen am 2. August 2026).

Voraussetzung. Das Fehlen des Wortes „geeignete" in § 13 Abs. 2 S. 1 KRITISDachG kann daher kein findiger Betreiber kritischer Anlagen einwenden.

4. Leerlaufende Wirtschaftlichkeitsklauseln in § 13 Abs. 2 KRITISDachG

Als Folgefehler des Risikobegriffs eröffnet das KRITIS-Dachgesetz scheinbar die Möglichkeit der Flucht in die sog. Zweck-Mittel-Relation, um Kosten zu vermeiden. Nach § 13 Abs. 2 S. 4 KRITISDachG gestattet der deutsche Gesetzgeber Betreibern kritischer Anlagen

> *(...) eine Zweck-Mittel-Relation vorzunehmen, bei der insbesondere der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls gegen das Risiko eines Vorfalls abzuwägen ist.*

§ 13 Abs. 2 S. 5 KRITISDachG ergänzt:

> *Wirtschaftliche Aspekte, darunter die Leistungsfähigkeit des Betreibers, sind zu berücksichtigen.*

Ein „Vorfall" (§ 2 Nr. 9 KRITISDachG) beeinträchtigt per definitionem eine „kritische Dienstleistung", deren Ausfall zu „erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit" führen würde (§ 2 Nr. 4 KRITISDachG). In der nach § 13 Abs. 2 S. 4 f. KRITISDachG gestatteten Abwägung stünden wirtschaftliche Interessen damit stets elementaren Sicherheits- und Versorgungsinteressen der Allgemeinheit gegenüber. Diese Abwägung kann ausweislich des KRITIS-Dachgesetzes, das via §§ 13 Abs. 2 S. 1, 11 Abs. 2 KRITISDachG gerade auch sog. High-Impact-Low-Probability-Ereignisse einbezieht, selbst nicht zugunsten des Betreibers einer kritischen Anlage ausgehen. § 13 Abs. 2 S. 4 f. KRITISDachG dürften daher in der Praxis ins Leere laufen.

II. Grundlagen und Begriffe des Risk Assessments

1. Gefahr („hazard") und Bedrohung („threat")

Ein Risk Assessment kommt nicht ohne „Gefahr" und „Bedrohung" aus. Während das KRITIS-Dachgesetz zu diesen Begriffen schweigt, ergibt sich die Relevanz von Gefahr

(„hazard") und Bedrohung („threat") aus der (englischsprachigen) Definition des „Risk Assessments" der CER-Richtlinie (Art. 2 Nr. 7 CER-RL).

Das „Risk Assessment" umfasst danach die jedem Risk Assessment notwendigerweise vorausgehende Gefahrenidentifikation[13] über die Risikoanalyse unter Einschluss der identifizierten Gefahren und Bedrohungen bis hin zur Risikobewertung, um eine informierte Entscheidung zur Risikobewältigung und Vertretbarkeit von (Gesamt-)Risiken zu ermöglichen. Die CER-Richtlinie definiert allerdings weder den Begriff der Gefahr noch den der Bedrohung.[14]

Eine Gefahr („hazard") bezeichnet im Allgemeinen die – mit einer Gefahrenquelle verbundene – Möglichkeit, einen Schaden herbeizuführen.[15] [16] Bei einer Gefahr handelt es sich um ein generelles Schadenspotenzial, unabhängig davon, ob oder mit welcher Wahrscheinlichkeit ein Schaden tatsächlich eintritt. Sie kann auch näher bestimmt werden, z.B. als anthropogene, technologische oder sozio-technologische Gefahr.[17] Das United Nations Office for Disaster Risk Reduction (UNDRR) hat im Jahr 2025 aktualisierte sog. Hazard Information Profiles als Ergänzung zum „UNDRR-ISC Hazard Definition and Classification Review: Technical report" aus dem Jahr 2020 herausgegeben.[18] Die HIPs umfassen 281 Gefahrenprofile, die nicht nur im Katastrophenmanagement, sondern auch im allgemeineren Resilienz-Kontext zur Orientierung herangezogen werden können.

Eine Bedrohung („threat") wird im Allgemeinen ebenfalls als eine Gefahr verstanden, die zusätzlich von menschlichem Schädigungswillen getragen ist, also z.B. eine

[13] Eine Risikoidentifikation ist nmA vor der Risikoanalyse nicht seriös möglich, daher wird hier von Gefahrenidentifikation gesprochen.
[14] Vielmehr vermengt sie wie andere EU-Rechtsakte, z.B. die KI-Verordnung (Verordnung (EU) 2024/1689), die Begriffe mit dem Begriff des Risikos.
[15] Vgl. United Nations Office for Disaster Risk Reduction (UNDRR), 2017, The Sendai Framework Terminology on Disaster Risk Reduction, „Hazard", abrufbar unter: https://www.undrr.org/terminology/hazard (zuletzt abgerufen am 2. August 2026).
[16] Lediglich beispielhaft für grundsätzlich vorhandenes EU-Gefahren- aber fehleranfälliges Risikoverständnis: EFSA, Europäische Behörde für Lebensmittelsicherheit, Gefahr-risiko (sic!), 15. Dezember 2023, abrufbar unter: https://www.efsa.europa.eu/de/campaigns/hazard-vs-risk (zuletzt abgerufen am 2. August 2026).
[17] Vgl. United Nations Office for Disaster Risk Reduction (UNDRR), 2017, The Sendai Framework Terminology on Disaster Risk Reduction, „Hazard", abrufbar unter: https://www.undrr.org/terminology/hazard (zuletzt abgerufen am 2. August 2026).
[18] United Nations Office for Disaster Risk Reduction (UNDRR), & International Science Council (ISC), 2025, UNDRR-ISC Hazard Information Profiles – 2025 Update, United Nations Office for Disaster Risk Reduction; International Science Council, abrufbar unter: https://doi.org/10.24948/2025.05 (zuletzt abgerufen am 2. August 2026).

terroristische Bedrohung. Oft wird der Begriff jedoch synonym mit dem Begriff der Gefahr verwendet.

Das KRITIS-Dachgesetz erfasst nach Vorstehendem v.a. in § 11 Abs. 2 KRITISDachG Gefahren und Bedrohungen, die lediglich fälschlich als „Risiken" benannt sind. Sie sind also Teil des Risk Assessments auch nach dem KRITIS-Dachgesetz.

Im Kontext von CER-Richtlinie und KRITIS-Dachgesetz ist insbesondere ein (Sicherheits-)Vorfall immer eine Gefahr. Dies legen bereits der Wortlaut des § 2 Nr. 9 KRITIS-DachG („ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen *könnte*"), die in Erwägungsgrund 5 CER-RL hervorgehobene Relevanz von Interdependenzen und Kaskadeneffekten sowie der in Erwägungsgrund 4 CER-RL geforderte Allgefahrenansatz („All-Hazards-Approach") nahe: Ein (Sicherheits-)Vorfall ist nie als isolierter Auslöser anzusehen, sondern stets als einer von vielen in Interdependenz zueinander stehenden (Sicherheits-)Vorfällen zu begreifen.

2. Vulnerabilität

Im Rahmen der Risikoanalyse als Teil des Risk Assessments erfolgt u.a. die Analyse der in der englischen Sprachfassung des Art. 2 Nr. 7 CER-RL genannten sog. Vulnerabilität. Sie erfasst die besondere Anfälligkeit oder Schutzbedürftigkeit exponierter Personen, Gruppen oder Systeme gegenüber Gefahren. Der Begriff der „Schwachstelle" in der deutschen Sprachfassung des Art. 2 Nr. 7 CER-RL ist demgegenüber in seiner Punktualität zu eng, um den maßgeblichen Einfluss der oft systemischen Vulnerabilität sowohl auf die Eintrittswahrscheinlichkeit als auch die Schwere eines Schadens erfassen zu können.

Da dieser Begriff jedoch aus der deutschen Sprachfassung der CER-Richtlinie übernommen wurde, die inhaltlich nicht von der englischen Sprachfassung abweichen kann, ist „Schwachstelle" hier einfach im weitesten Sinne als Vulnerabilität zu verstehen.

III. Risiko vs. Resilienz

Das Risiko ist das Ergebnis des Risk Assessments und die Grund- und Ausgangslage für Maßnahmen der Risikobewältigung (auch: Risikomanagement genannt).

Die Resilienz ist wiederum das Ergebnis der Risikobewältigung auf der Grundlage des Risk Assessments. In der Folge verfügt der Betreiber einer kritischen Anlage über die (Handlungs-) Fähigkeit im Sinne des § 2 Nr. 5 KRITISDachG,

1. einen Vorfall zu verhindern,
2. sich vor einem Vorfall zu schützen,
3. einen Vorfall abzuwehren,
4. auf einen Vorfall zu reagieren,
5. die Folgen eines Vorfalls zu begrenzen,
6. einen Vorfall aufzufangen und
7. zu bewältigen und
8. sich von einem Vorfall zu erholen.

Da das Risk Assessment ausweislich der Relevanz dynamischer und kaskadierender Bedrohungen (vgl. Erwägungsgrund 3 CER-RL) ein iterativer Gesamtprozess ist, kann auch die so verstandene Resilienz kein statischer Zustand sein, erst recht kein Zustand einer Anlage. Resilienz erfordert daher die fortlaufende Anpassung der (Schutz-)Maßnahmen an das fortlaufend zu aktualisierende Risikobild.

C. Anforderungen an den Inhalt des Resilienzplans

I. Formale Anforderungen an den Resilienzplan

Die wichtigsten allgemeinen Anforderungen an den Resilienzplan sind formaler Natur:

Nach § 13 Abs. 4 iVm Abs. 1 bis 3 KRITISDachG müssen die zur Herstellung der Resilienz erforderlichen Maßnahmen auf der Grundlage eines Risk Assessments getroffen werden, welches im Resilienzplan in den wesentlichen Zügen darzustellen, mindestens aber in Bezug zu nehmen ist. Aus dem Resilienzplan ergeben sich diese Maßnahmen in umsetzbarer Art und Weise. Die Gründe für ihre Auswahl im Kontext des Risk Assessments müssen ebenfalls aus dem Plan hervorgehen. Somit muss sich aus ihm die (Handlungs-)Fähigkeit Resilienz, die in § 2 Nr. 5 KRITISDachG konkretisiert wird, entnehmen lassen.

Die Vorlage des Resilienzplans kann von der zuständigen Behörde nach § 16 Abs. 2 S. 2 KRITISDachG verlangt werden. Er sollte daher in Vorbereitung einer behördlichen Einsichtnahme verfasst und gestaltet werden, folglich mit Blick auf die damit u.a. nachzuweisende (Handlungs-)Fähigkeit Resilienz nachvollziehbar sein. Da das Risk Assessment iterativ ist und wohl auch die Beseitigung von Mängeln des Resilienzplans nach § 16 Abs. 5 iVm Abs. 2 S. 2 KRITISDachG behördlich verlangt werden kann, sollte der Resilienzplan in einer anpassungstauglichen Form vorgehalten werden.

§ 13 Abs. 4 KRITISDachG verlangt einen „Resilienzplan". Art. 13 Abs. 2 S. 1 CER-RL gestattet jedoch ausdrücklich „ein gleichwertiges Dokument oder Dokumente", auch um auf bereits bestehenden Unterlagen aufbauen zu können und Doppelarbeit zu vermeiden (vgl. Art. 13 Abs. 2 S. 2 CER-RL). Die Verwendung von Vorlagen und Mustern für die Erstellung von Resilienzplänen nach § 13 Abs. 5 KRITISDachG ist gesetzlich nicht verbindlich vorgeschrieben, sodass sich auch hieraus die Formfreiheit entsprechend Art. 13 Abs. 2 S. 1 CER-RL ergeben dürfte. Die Umsetzung einer richtlinienkonformen Auslegung in Abkehr von den formalen Anforderungen des KRITIS-Dachgesetzes sollte allerdings erst nach Rücksprache mit der zuständigen Behörde erfolgen. Um dies zu verdeutlichen, wird hier stets vom Resilienzplan gesprochen.

II. Inhaltliche Anforderungen an den Resilienzplan

Das KRITIS-Dachgesetz wie auch die CER-Richtlinie enthalten aus guten Gründen keine konkreten Vorgaben an den Inhalt eines Resilienzplans. Betreiber kritischer Anlagen sollen die gesetzlichen Anforderungen einzelfallgerecht erfüllen können. Wie so oft bringen große Freiheiten aber auch Unsicherheit mit sich, weil die Erwartungen vielgestaltig erfüllt werden können. Orientierung tut hier im Sinne der Resilienzziele Not.

1. Der Resilienzplan-Algorithmus

Bei dem Resilienzplan handelt es sich nicht nur um ein Dokument, sondern vielmehr um eine Resilienzplanung im Sinne eines dokumentierten, iterativen Prozesses. Vorlagen oder Muster nach § 13 Abs. 5 KRITISDachG können hilfreich, aber auch hinderlich sein, wenn sie besonders umfangreich, detailliert und nicht einzelfallgerecht ausfallen.

Daher wird hier ein „Resilienzplan-Algorithmus" vorgeschlagen, den Betreiber kritischer Anlagen der Entwicklung ihrer Resilienzplanung einschließlich ihres Resilienzplans unter Berücksichtigung der in den Abschnitten A. und B. ausgeführten Aspekte zugrunde legen können. Er dient als Methodik oder Framework, um durch Systematik, Regelhaftigkeit und Regelmäßigkeit Komplexität auch z.B. im Sinne einer Interoperabilität über die Organisation hinaus handhabbar zu machen. Die vereinfachende, abstrahierende Bezeichnung soll diese Funktion verdeutlichen. Da der Resilienzplan-Algorithmus zudem leicht zu merken und zu vermitteln ist, wird nicht zuletzt die Einarbeitung neuer Mitwirkender erleichtert.

Der Resilienzplan-Algorithmus übersetzt die Iterativität der Resilienzplanung im Sinne von CER-Richtlinie und KRITIS-Dachgesetz durch Anwendung des PDCA-Zyklus und kombiniert ihre Phasen mit bekannten Business-Continuity- sowie Projektmanagement-Anforderungen. So wird zum einen die Resilienzplanung erheblich erleichtert. Zum anderen wird damit die in Art. 13 Abs. 2 S. 2 CER-RL hergestellte Verbindung zu Verfahren nach anderen Rechtsakten sowie die in § 13 Abs. 2 S. 2 KRITISDachG nach Maßgabe von Art. 16 CER-RL hervorgehobene Bedeutung von relevanten europäischen und internationalen Normen und technischen Spezifikationen unterstützt.

Betreiber kritischer Anlagen legen auf dieser Grundlage einzelfallgerecht die Details ihrer Resilienzplanung fest und ermöglichen damit insbesondere die Erstellung und Anwendung eines Resilienzplans.

Der Resilienzplan-Algorithmus mit den iterativen Phasen Plan-Do-Check-Act (PDCA) lässt sich wie folgt darstellen:

a. (Neu-)Konzeption für X (*Plan*)

Festgelegt werden hier anhand der Fragestellung: *„Wer macht was, womit, wie, warum und mit welchem Ziel?"* die Grundlagen oder Rahmenbedingungen, damit eine Resilienzplanung überhaupt möglich ist:

1. Rollen & Ressourcen: Verantwortlichkeiten und Zuständigkeiten sowie Allokation der benötigten Ressourcen (z.B. Personal, Zeit und Mittel).
2. Prozesse & Schnittstellen: Allgemeine Verfahren, Anforderungen, Vorgehensweisen und Schnittstellen (z.B. zum Risk Assessment).
3. Vorgaben & Ziele: Rechtliche wie tatsächliche Maßstäbe (s.o.), Methodiken und Methoden sowie Zielvorgaben, die u.a. die Evaluierung ermöglichen.

b. Operationalisierung für X (*Do*)

Festgelegt werden hier anhand der Fragestellung: *„Wie wird entschieden, umgesetzt, informiert und kommuniziert?"* die Bedingungen, welche die Resilienzplanung praktisch umsetzbar und damit anwendbar machen:

1. Selektion & Priorisierung: Besondere Verfahren und Anforderungen wie z.B. Auswahlkriterien (etwa Priorisierungsregeln bei Ressourcenknappheit).
2. Umsetzung & Dokumentation: Besondere Verfahren und Anforderungen an die Umsetzung sowie Dokumentation.
3. Information & Kommunikation: Besondere Verfahren und Anforderungen z.B. an Berichte und Zugangsbefugnisse (etwa iSd Need-to-know-Prinzips).

c. Evaluierung für X (*Check*)

Festgelegt werden hier anhand der Fragestellung: „*Wie wird objektiv und transparent gemessen?*" die Bedingungen, welche die Resilienzplanung überprüf- sowie verbesserbar machen:

1. Messung & Abgleich: Besondere Verfahren und Anforderungen zu Überprüfungszwecken (z.B. Soll-Ist-Abgleiche).
2. Unabhängigkeit & Qualität: Besondere Verfahren und Anforderungen zur Qualitätssicherung und Vermeidung von Interessenkonflikten (z.B. durch Funktionstrennung).
3. Reporting & Transparenz: Besondere Verfahren und Anforderungen z.B. im Kontext der Informationsbereitstellung intern wie extern, einschließlich gegenüber der zuständigen Behörde.

d. Anpassung für X (*Act*)

Festgelegt werden hier anhand der Fragestellung: „*Wie wird gelernt und nachgebessert?*" die Bedingungen, welche die Resilienzplanung als Prozess iterativ machen:

1. Auslöseereignisse & Eskalation: Besondere Verfahren und Anforderungen wie z.B. Schwellenwerte, Eskalationswege und Umsetzungsfristen.
2. Evolution & Nachbereitung: Besondere Verfahren und Anforderungen an die systematische Fortschreibung (z.B. Lessons Learned nach Vorfällen).
3. Korrektur & Nachverfolgung: Besondere Verfahren und Anforderungen z.B. an Änderungen, Änderungsnachverfolgung und Änderungskommunikation.

2. Allgemeiner Teil des Resilienzplans

a. Grundsätzliches

Die Resilienzplanung erfordert nach dem KRITIS-Dachgesetz eine nachweisbare Dokumentation („Resilienzplan"), auch um behördliche Überprüfungen zu ermöglichen.

Der Allgemeine Teil des Resilienzplans beschreibt im Wesentlichen das Betriebssystem, auf dessen Grundlage die Resilienz als Gesamtheit organisationaler (Handlungs-)Fähigkeit(en) entstehen, bestehen und fortbestehen kann. Er ist erforderlich, um den Grundstein für diese Befähigung zu legen und sicherzustellen, dass die Anforderungen an die Resilienzplanung durch gute (Corporate) Governance stets eingehalten werden können.

b. Resilienzplan-Algorithmus

Der Resilienzplan-Algorithmus mit den iterativen Phasen Plan-Do-Check-Act (PDCA) lässt sich für den Allgemeinen Teil des Resilienzplans (die Governance-Ebene) als Dokument oder Dokumentation wie folgt anwenden:

aa. (Neu-)Konzeption des Resilienzplans (*Plan*)

Festgelegt werden anhand der Fragestellung: *„Wer macht was, womit, wie, warum und mit welchem Ziel?"* die Grundlagen oder Rahmenbedingungen, damit ein Resilienzplan überhaupt erstellt und fortgeschrieben werden kann:

1. Rollen & Ressourcen: Verantwortlichkeiten und Zuständigkeiten sowie Allokation der benötigten Ressourcen (z.B. Personal, Zeit und Mittel).
2. Prozesse & Schnittstellen: Allgemeine Verfahren, Anforderungen, Vorgehensweisen und Schnittstellen (z.B. zum Risk Assessment).
3. Vorgaben & Ziele: Rechtliche wie tatsächliche Maßstäbe (s.o.), Methodiken und Methoden sowie Zielvorgaben, die u.a. die Evaluierung ermöglichen.

bb. Operationalisierung des Resilienzplans (*Do*)

Festgelegt werden anhand der Fragestellung: *„Wie wird entschieden, umgesetzt, informiert und kommuniziert?"* die Bedingungen, welche den Resilienzplan praktisch umsetzbar und damit anwendbar machen:

1. Selektion & Priorisierung: Besondere Verfahren und Anforderungen wie z.B. Auswahlkriterien (etwa Priorisierungsregeln bei Ressourcenknappheit).

2. Umsetzung & Dokumentation: Besondere Verfahren und Anforderungen an die Umsetzung sowie Dokumentation.
3. Information & Kommunikation: Besondere Verfahren und Anforderungen z.B. an Berichte und Zugangsbefugnisse (etwa iSd Need-to-know-Prinzips).

cc. Evaluierung des Resilienzplans (*Check*)

Festgelegt werden anhand der Fragestellung: *„Wie wird objektiv und transparent gemessen?"* die Bedingungen, welche den Resilienzplan überprüf- sowie verbesserbar machen:

1. Messung & Abgleich: Besondere Verfahren und Anforderungen zu Überprüfungszwecken (z.B. Soll-Ist-Abgleiche).
2. Unabhängigkeit & Qualität: Besondere Verfahren und Anforderungen zur Qualitätssicherung und Vermeidung von Interessenkonflikten (z.B. durch Funktionstrennung).
3. Reporting & Transparenz: Besondere Verfahren und Anforderungen z.B. im Kontext der Informationsbereitstellung intern wie extern, einschließlich gegenüber der zuständigen Behörde.

dd. Anpassung des Resilienzplans (*Act*)

Festgelegt werden anhand der Fragestellung: *„Wie wird gelernt und nachgebessert?"* die Bedingungen, welche den Resilienzplan nachbesserbar machen:

1. Auslöseereignisse & Eskalation: Besondere Verfahren und Anforderungen wie z.B. Schwellenwerte, Eskalationswege und Umsetzungsfristen.
2. Evolution & Nachbereitung: Besondere Verfahren und Anforderungen an die systematische Fortschreibung (z.B. Lessons Learned nach Vorfällen).
3. Korrektur & Nachverfolgung: Besondere Verfahren und Anforderungen z.B. an Änderungen, Änderungsnachverfolgung und Änderungskommunikation.

3. Besonderer Teil des Resilienzplans

a. Grundsätzliches

Der Besondere Teil des Resilienzplans dient dann wie Anwendersoftware dazu, die konkreten Maßnahmen nach § 13 Abs. 1 bis 3 KRITISDachG bzw. Art. 13 Abs. 1 CER-RL umzusetzen und damit den Resilienzplan anzuwenden (vgl. § 13 Abs. 4 S. 1 KRITISDachG und Art. 13 Abs. 2 S. 1 CER-RL).

b. Resilienzplan-Algorithmus

Die Anwendung des Resilienzplan-Algorithmus auf die einzelnen Maßnahmenkategorien fördert eine einheitliche Struktur und damit Klarheit wie auch Nachvollziehbarkeit. Am Beispiel der Kategorie „Prävention von Vorfällen" (nach Vorbild von Art. 13 Abs. 1 lit. a CER-RL und § 13 Abs. 1 Nr. 1 KRITISDachG) stellt sich die Anwendung wie folgt dar:

aa. (Neu-)Konzeption von Prävention (*Plan*)

Festgelegt werden anhand der Fragestellung: *„Wer macht was, womit, wie, warum und mit welchem Ziel?"* die Grundlagen oder Rahmenbedingungen, damit die Prävention von Vorfällen überhaupt ermöglicht werden kann:

1. **Rollen & Ressourcen:** Verantwortlichkeiten und Zuständigkeiten sowie Allokation der benötigten Ressourcen (z.B. Personal, Zeit und Mittel).
2. **Prozesse & Schnittstellen:** Allgemeine Verfahren, Anforderungen, Vorgehensweisen und Schnittstellen (z.B. zum Risk Assessment).
3. **Vorgaben & Ziele:** Rechtliche wie tatsächliche Maßstäbe (s.o.), Methodiken und Methoden sowie Zielvorgaben, die u.a. die Evaluierung ermöglichen.

bb. Operationalisierung der Präventionsmaßnahmen (*Do*)

Festgelegt werden anhand der Fragestellung: *„Wie wird entschieden, umgesetzt, informiert und kommuniziert?"* die Bedingungen, welche die Präventionsmaßnahmen praktisch umsetzbar und damit anwendbar machen:

1. Selektion & Priorisierung: Besondere Verfahren und Anforderungen wie z.B. Auswahlkriterien (etwa Priorisierungsregeln bei Ressourcenknappheit).
2. Umsetzung & Dokumentation: Besondere Verfahren und Anforderungen an die Umsetzung sowie Dokumentation.
3. Information & Kommunikation: Besondere Verfahren und Anforderungen z.B. an Berichte und Zugangsbefugnisse (etwa iSd Need-to-know-Prinzips).

cc. Evaluierung der Präventionsmaßnahmen (*Check*)

Festgelegt werden anhand der Fragestellung: *„Wie wird objektiv und transparent gemessen?"* die Bedingungen, welche die Präventionsmaßnahmen überprüf- sowie verbesserbar machen:

1. Messung & Abgleich: Besondere Verfahren und Anforderungen zu Überprüfungszwecken (z.B. Soll-Ist-Abgleiche).
2. Unabhängigkeit & Qualität: Besondere Verfahren und Anforderungen zur Qualitätssicherung und Vermeidung von Interessenkonflikten (z.B. durch Funktionstrennung).
3. Reporting & Transparenz: Besondere Verfahren und Anforderungen z.B. im Kontext der Informationsbereitstellung intern wie extern, einschließlich gegenüber der zuständigen Behörde.

dd. Anpassung der Präventionsmaßnahmen (*Act*)

Festgelegt werden anhand der Fragestellung: *„Wie wird gelernt und nachgebessert?"* die Bedingungen, welche die Präventionsmaßnahmen nachbesserbar machen:

1. Auslöseereignisse & Eskalation: Besondere Verfahren und Anforderungen wie z.B. Schwellenwerte, Eskalationswege und Umsetzungsfristen.
2. Evolution & Nachbereitung: Besondere Verfahren und Anforderungen an die systematische Fortschreibung (z.B. Lessons Learned nach Vorfällen).
3. Korrektur & Nachverfolgung: Besondere Verfahren und Anforderungen z.B. an Änderungen, Änderungsnachverfolgung und Änderungskommunikation.

Über die Autorin

Rechtsanwältin Claudia Otto, MBA, ist Expertin für Sicherheits- und Katastrophenmanagement sowie Dozentin für Corporate Governance. An der University of Oxford lehrt sie zudem als Gastdozentin zu Recht und Ethik im Kontext der Nutzung Generativer KI im Finanzbereich. Sie zeigt auf, wie Organisationen resilient werden und damit in Extremlagen handlungsfähig bleiben. Ihr systemischer Ansatz ermöglicht es, ausbremsende Silostrukturen zu überwinden.

Aus dem Anliegen heraus, die Resilienz kritischer Einrichtungen nachhaltig zu stärken, übersetzt sie u.a. komplexe rechtliche Vorgaben in verständliche, direkt anwendbare Orientierungshilfen. Als Rechtsanwältin unterstützt sie Gesetzesadressatinnen und Gesetzesadressaten sowie Organisationen dabei, ihr Handeln rechtssicher auszurichten, rechtliche Anforderungen praxistauglich zu bewältigen und allgemeine wie maßgeschneiderte Resilienzrahmen im Einklang mit dem Recht auszufüllen.