C]A

STANDARD

C]ORE Standard

Managementsystem für
organisationale Krisenresilienz

01	VERSION 1.0
02	STAND: JUNI 2026
03	RICO KERSTAN / PROF. DR. ANDRÉ RÖHL
04	OPEN SOURCE STANDARD

Inhalt

ZITIERVORSCHLAG

Kerstan, Rico/Röhl, André: C]A-Standard C]ORE. Managementsystem für organisationale Krisenresilienz, Version 1.0, Stand: Juni 2026, Crisis Architecture, 2026.

1 Einleitung

Krisen der jüngeren Vergangenheit zeigen auf, wie vulnerabel unsere digitalisierte Gesellschaft ist. Organisationen müssen Handlungsoptionen entwickeln, um mit den Auswirkungen komplexer Ereignisse umzugehen. Um die Resilienz unserer Gesellschaft auch in Zeiten großer Ungewissheit zu steigern, bedarf es Mut, die Verantwortlichkeiten für Krisenvorsorge und -bewältigung neu zu denken. Oberstes Ziel der Vorbereitungen ist die Wahrung der Handlungs- und Entscheidungsfähigkeit. Für Organisationen bedeutet dies, dass sie sich im Rahmen der allgemeinen Gefahrenabwehr auf die vielschichtigen Auswirkungen vorbereiten müssen.

Die Covid-19-Pandemie hat zudem gezeigt, dass die Legaldefinition von Kritischen Infrastrukturen (KRITIS) in einer umfassenden Krise nur wenig hilfreich ist. Beispielsweise fallen von rund 2000 Krankenhäusern in Deutschland nur knapp 200 unter die gesetzliche KRITIS-Definition nach BSIG. Für die einzelne Organisation ist ein Krankenhaus aber dennoch von großer Bedeutung. Zudem müssen die kommunalen Organisationen selbst als kritisches Element verstanden werden, sind diese doch wichtiger Teil der örtlichen Gemeinschaft. Aber auch Ad-Hoc-Auslegungen zur „Systemrelevanz" waren in der Vergangenheit im Ergebnis zu ungenau, um daraus eine zielgerichtete Vorbereitung auf kommunaler Ebene abzuleiten.

In den jüngeren Krisen, z. B. der Corona-Pandemie sowie dem Hochwasser im Ahrtal, wurde deutlich, dass die steigende Vernetzung der Gesellschaft durch digitale Medien und die schnelle Verbreitung von Informationen zu neuen Modellen der Kooperation bei der Krisenbewältigung führen oder bereits bekannte Modelle intensivieren. Hier sind vor allem zwei Arten der Kooperation zu nennen: interorganisationale Kooperation, bei der sich mehrere Organisationen zum Zwecke der Krisenbewältigung zusammenschließen sowie die individuelle Kooperation einzelner Menschen oder Initiativen, die sich in die Bewältigung von Krisen bzw. Katastrophen einbringen. Aktuelle wissenschaftliche Erkenntnisse untermauern, dass Organisationen jeder Größe positive Effekte der Kooperation erfahren. Je mehr Partner Teil der Kooperation sind und je diverser die Beteiligten sind, desto mehr Wissen stehe allen Partnern zur Verfügung.

Organisationen sollten daher die Krisenresilienz in das Zentrum der Vorbereitungen auf künftige Krisen stellen. Das dem C]ORE®-Ansatz zugrunde liegende Resilienzmodell unterscheidet hierbei vier Handlungsfelder organisationaler Krisenresilienz:

- Widerstandsfähigkeit (Verringerung von Risiken und Schäden),
- Bewältigungsfähigkeit (Überwindung des Schadens),
- Verständnis des inneren Ökosystems (organisationsspezifisches Handeln im Unternehmen),
- Verständnis des äußeren Ökosystems (organisationsspezifisches Handeln innerhalb des eigenen lokalen, regionalen und überregionalen Netzwerkes).

Corporate Organizational Resilience Excellence (C]ORE®) ist ein Konzept, das sich auf die Fähigkeit von Organisationen bezieht, geplante, unerwartete und neue Herausforderungen zu überstehen, indem das innere und äußere Ökosystem aktiv als Ressourcenquelle für die Krisenprävention und -bewältigung verstanden wird. C]ORE® bedingt ein hohes Maß an Widerstands- und Bewältigungsfähigkeit von der Organisation und vom äußeren Ökosystem, um die Funktionsfähigkeit auch bei akuten Bedrohungen und Herausforderungen aufrechtzuerhalten und im Anschluss in einen stabilen Zustand zurückzukehren. Zudem bedarf C]ORE® eines hohen Maßes an Verständnis über das Ökosystem innerhalb der Organisation und der eigenen lokalen, regionalen und überregionalen Netzwerke.

C]ORE® umfasst die Vorbeugung, die Überwachung, die Bewältigung von Störungen und Krisen sowie die Wiederherstellung und den Wiederanlauf nach solchen Ereignissen. Hierzu gehören vielfältige Kompetenzen und Methoden, unter anderem die Fähigkeit, Risiken zu erkennen und zu bewerten, die Entwicklung und Implementierung von Reaktionsplänen, die Durchführung von Übungen und Schulungen sowie die Fähigkeit, schnell auf Krisensituationen zu reagieren.

C]ORE® liefert Organisationen ein fundiertes Lagebild zu Potenzialen, aber auch Schwächen in den eigenen Strukturen und im äußeren Ökosystem. Das Konzept ist Voraussetzung für eine zielgerichtete Steuerung von Ressourcen im Krisenfall, für Investitionen und für die Förderung organisationaler Krisenresilienz.

C]ORE® macht Krisenbewältigung zum gesellschaftlichen Gemeinschaftsprojekt. Auch trotz neuartiger Bedrohungs- und Krisenszenarien kann auf diese Weise die unverzichtbare Kompetenz der Organisation zur Lösung von Krisen zur Geltung gebracht werden.

2 Allgemeines

2.1 Nutzungshinweise

Der vorliegende C]A-Standard orientiert sich an internationalen Normen sowie aktuellen Erkenntnissen der Forschung zu organisationaler Resilienz. Er beschreibt ein Managementsystem für Organisationen, das dem C]ORE®-Ansatz folgt. Organisationen, die den Standard umgesetzt haben, können die Zertifizierung nach Crisis Architecture beantragen. Die Zertifizierung erfolgt über lizenzierte Zertifizierungsstellen und unabhängige Prüfer.

Die Implementierung eines C]ORE®-Managementsystems stellt eine wichtige strategische Entscheidung für eine Organisation dar. Gestaltung und Umsetzung des C]ORE®-Managementsystems müssen sich an den Bedürfnissen, Zielen, Anforderungen, Abläufen und der Größe der Organisation orientieren. Da sich diese Faktoren im Laufe der Zeit verändern können, ist es wichtig, dass das C]ORE®-Managementsystem regelmäßig überprüft wird.

Es ist von Bedeutung, dass das C]ORE®-Managementsystem in Prozesse und die Aufbauorganisation der Organisation integriert ist und bei der Organisationsentwicklung wie auch der Weiterentwicklung der Strategie berücksichtigt wird. Die Umsetzung des C]ORE®-Managementsystems sollte flexibel an die Bedürfnisse der Organisation angepasst werden.

Dieser Standard kann von Aufsichtsbehörden, Mitarbeitern, Lieferanten und interessierten Organisationen genutzt werden, um organisationale Krisenresilienz einer Organisation zu bewerten.

Die Nummerierung der Anforderungen in diesem Standard spiegelt weder ihre Bedeutung noch die Umsetzungsreihenfolge wider.

Das Kennzeichen „#KRITISDACHG“ verweist in diesem Standard auf Anforderungen, Hinweise oder Maßnahmen mit spezifischem Bezug zur Umsetzung des KRITIS-Dachgesetzes. Die Kennzeichnung ersetzt keine rechtliche Prüfung. Sie unterstützt Organisationen dabei, einschlägige Anforderungen zum Betreiberstatus, zur Risikoanalyse, zum Resilienzplan, zu Nachweisen, Audits und Meldungen im C]ORE®-Managementsystem nachvollziehbar zu berücksichtigen.

2.2 Anwendungs- und Geltungsbereich

Dieser C]A-Standard legt Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines C]ORE®-Managementsystems für Organisationen jeder Art und Größe fest. Der Standard kann insbesondere von kritischen Infrastrukturen angewendet werden.

2.3 Änderungshistorie

Dies ist die erste Version des C]A-Standards.

3 Begriffe

3.1 Ausfallwirkung

Eine Ausfallwirkung umfasst Folgen oder Konsequenzen, die entstehen, wenn ein System, ein Prozess, eine Komponente oder eine Funktion nicht wie erwartet funktioniert oder ausfällt.

3.2 Bewältigungsfähigkeit

Fähigkeit einer Organisation und ihrer Bestandteile, Herausforderungen und Stressoren infolge einer Abweichung vom Normalzustand erfolgreich zu bewältigen und in einer sicheren und effektiven Art und Weise zu reagieren.

3.3 Dokumentierte Information

Information, die von einer Organisation gelenkt und aufrechterhalten werden muss (ISO 9000:2015, 3.8.6).

3.4 Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen (ISO 9000:2015, 3.7.1).

3.5 Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen (ISO 9000:2015, 3.1.6).

3.6 Kontinuitätsplanung

Prozess, bei dem Organisationen Maßnahmen planen, festlegen und implementieren, um sicherzustellen, dass ihre operative Tätigkeit auch in Zeiten von Unterbrechungen oder Störungen aufrechterhalten werden kann.

3.7 Kooperationsplanung

Prozess der Überlegung und Vereinbarung von Zielen, Aufgaben und Verantwortlichkeiten zwischen zwei oder mehreren Parteien, die zusammenarbeiten möchten, um gemeinsame Projekte oder Ziele zu erreichen.

3.8 Krise

Vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden an Schutzgütern, die mit der normalen Aufbau- und Ablauforganisation nicht mehr bewältigt werden kann, so dass eine besondere Aufbauorganisation erforderlich ist (vgl. Glossar des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe).

3.9 Krisenmanagement

Alle Maßnahmen zur Vorbereitung auf Erkennung und Bewältigung, Vermeidung weiterer Eskalation sowie Nachbereitung von Krisen (vgl. Glossar des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe).

3.10 Kritikalitätsstufe

Grad der Bedeutung oder Dringlichkeit, die einem bestimmten Aspekt zugewiesen wird. Objektives Maß für die Wichtigkeit von Aufgaben, Prozessen, Organisationen oder Systemen.

3.11 Kritische Infrastrukturen

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (vgl. KRITIS-Definition der Bundesressorts).

3.12 Oberste Leitung

Person oder Personengruppe, die eine Organisation auf der obersten Ebene leitet und lenkt.

3.13 Lieferkette

Netzwerk von Organisationen, Personen und Aktivitäten, die notwendig sind, um ein Produkt oder eine Dienstleistung von den Ursprüngen bis zum Endkunden zu produzieren und zu liefern.

3.14 Managementsystem

Satz zusammenhängender oder sich gegenseitig beeinflussender Elemente einer Organisation, um Politiken, Ziele und Prozesse zum Erreichen dieser Ziele festzulegen (vgl. ISO 9000:2015, 3.5.3).

3.15 Organisationale Resilienz

Vermögen einer Organisation und ihrer Bestandteile, geplante, unerwartete und neue Ereignisse zu überstehen. Organisationale Resilienz bedingt eine Widerstandsfähigkeit (vgl. 3.25) sowie eine Bewältigungsfähigkeit (vgl. 3.2).

3.16 Organisationen mit Einfluss auf die Resilienz

Institutionen, Unternehmen oder Vereinigungen, die eine Rolle bei der Stärkung oder Schwächung der Widerstands- und Bewältigungsfähigkeit haben.

3.17 Risikobeurteilung

Prozess, bei dem mögliche Bedrohungen und die damit verbundenen Risiken für eine Organisation identifiziert, bewertet und beurteilt werden. Der Zweck der Risikobeurteilung ist es, die wahrscheinlichen Auswirkungen von Risiken zu bestimmen und Maßnahmen zur Minimierung oder Vermeidung dieser Risiken zu ergreifen.

Anmerkung: ISO 31000 stellt ein generisches Vorgehen für Risikobeurteilungen vor.

3.18 Schadensszenario

Ereignis oder Zustand mit negativen Auswirkungen auf ein Unternehmen, eine Organisation oder eine Gesellschaft. Diese Auswirkungen können finanziell, operativ, reputationsbedingt oder in anderer Weise erfolgen. Schadensszenarien können aufgrund von Naturkatastrophen, technischen Störungen, menschlichem Versagen, kriminellen Handlungen oder anderen Faktoren entstehen.

3.19 Störfallbetriebe

Betriebe, für die die Störfall-Verordnung Anwendung findet. Es handelt sich um Infrastrukturen, in denen gefährliche Stoffe in Mengen vorhanden sind, die definierte Mengenschwellen überschreiten.

3.20 Störung

Unerwartetes Ereignis oder unerwarteter Zustand mit geringfügiger Unterbrechung oder Beeinträchtigung normaler Betriebsabläufe.

3.21 Unterstützungsbedürftigkeit

Fähigkeit einer Organisation oder einer Person, ihre grundlegenden Bedürfnisse und Anforderungen ohne externe Hilfe zu befriedigen.

3.22 Unterstützungspotential

Fähigkeit einer Person oder Organisation, anderen Personen, Gruppen oder Organisationen Unterstützung zu bieten. Unterstützungspotential kann unter anderem in Bezug auf finanzielle Mittel, Fachwissen, Ressourcen und Zeit bestimmt werden.

3.23 Widerstandsfähigkeit

Fähigkeit einer Organisation und ihrer Bestandteile, den Eintritt einer Krise zu verhindern oder zu verzögern.

3.24 Wirkungskette

Abfolge von Ereignissen, die aus einem bestimmten Auslöser resultieren. Eine Wirkungskette zeigt die Wechselwirkungen und Abhängigkeiten zwischen verschiedenen Elementen und Einflussfaktoren auf und verfolgt die Auswirkungen einer Veränderung entlang einer Kette von Ursache und Wirkung.

3.25 Wirtschaftsstabilität

Fähigkeit einer Organisation wirtschaftlichen Herausforderungen standzuhalten und sich davon zu erholen. Wirtschaftsstabilität beinhaltet den Umgang mit Schwankungen oder Schocks in der Wirtschaft, wie z. B. Rezessionen, Finanzkrisen oder plötzliche Veränderungen der Marktnachfrage. Dies beinhaltet robuste Geschäftsmodelle, solide Finanzierungsstrategien, Diversifizierung von Einnahmequellen und die Fähigkeit, schnell auf sich verändernde Umstände zu reagieren.

4 Umfeldanalyse

4.1 Verstehen des Ökosystems

ANF4.1 Die Organisation muss externe und interne Themen identifizieren, die für sie und ihre strategische Ausrichtung relevant sind und ihre organisationale Resilienz beeinflussen.

ANF4.2 Die Organisation muss die zutreffenden gesetzlichen, behördlichen und selbstauferlegten Anforderungen bestimmen, die sich auf ihre organisationale Resilienz beziehen.

ANF4.3 Die Organisation muss relevante Schadensszenarien identifizieren, die Auswirkungen auf ihre organisationale Resilienz haben.

ANF4.4 Die Organisation muss Informationen über diese externen und internen Themen fortlaufend überwachen und überprüfen.

ANF4.5 Die Ergebnisse müssen als dokumentierte Informationen aufbewahrt werden.

4.2 Analyse der Organisationen mit Einfluss auf die Resilienz

ANF4.6 Aufgrund ihrer Bedeutung für die organisationale Resilienz für die Organisation, muss sie

1. die relevanten Organisationen mit Einfluss auf die Resilienz,
2. die für die organisationale Resilienz relevanten Erwartungen an die Organisation sowie
3. die für die organisationale Resilienz der Organisation relevanten Einflüsse auf das äußere Ökosystem bestimmen.

> Der Einfluss der Organisation auf betroffene Gebietskörperschaften, kritische Infrastrukturen und Störfallbetriebe muss explizit berücksichtigt werden.

ANF4.7 Die Organisation muss die Erwartungen und Einflüsse in resilienzfördernde und resilienzschwächende Aspekte einteilen.

ANF4.8 Die Analyse muss die tatsächlichen Wirkungsketten berücksichtigen.

> *ANMERKUNG: In Einzelfällen können die tatsächlichen Wirkungsketten über die Organisationsgrenzen hinausgehen (z. B. bei Outsourcing).*

ANF4.9 Die Organisation muss die Erwartungen und Einflüsse fortlaufend überwachen und überprüfen.

ANF4.10 Die Ergebnisse müssen als dokumentierte Informationen aufbewahrt werden.

4.3 Festlegen des Anwendungsbereichs

ANF4.11 Die Organisation muss die Grenzen und die Anwendbarkeit ihres C]ORE®-Managementsystems festlegen.

ANF4.12 Bei der Festlegung dieses Anwendungsbereichs muss die Organisation

1. das unter 4.1 genannte Ökosystem inklusive der betrachteten Schadensszenarien,
2. die unter 4.2 genannte Analyse der Organisationen mit Einfluss auf die Resilienz und
3. die organisationalen Besonderheiten berücksichtigen.

ANF4.13 Die Organisation muss sämtliche Anforderungen dieses Standards anwenden, wenn sie innerhalb des festgelegten Anwendungsbereichs ihres C]ORE®-Managementsystems anwendbar sind. Für jede Anforderung dieses Standards, die von der Organisation als nichtzutreffend bestimmt wird, muss eine ausführliche Begründung dokumentiert werden.

ANF4.14 Der Anwendungsbereich des C]ORE®-Managementsystems der Organisation muss als dokumentierte Information verfügbar sein und aufrechterhalten werden.

> *Hinweis #KRITISDACHG: Organisationen, die kritische Dienstleistungen erbringen oder Anlagen mit erheblicher Bedeutung für kritische Dienstleistungen betreiben, sollten im Rahmen von 4.3 einen dokumentierten KRITIS-DachG-Anwendbarkeitscheck durchführen. Zu prüfen sind insbesondere Betreiberstatus und bestimmender Einfluss, Zuordnung zu Sektoren und Ausnahmen, Erheblichkeit der Anlage, Registrierungspflichten und Übergangsregelungen nach §§ 2, 4, 5, 8 und 26 KRITIS-DachG.*

4.4 Prozesse für das C]ORE®-Managementsystem

ANF4.15 Die Organisation muss entsprechend den Anforderungen dieses Standards ein C]ORE®-Managementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihrer Wechselwirkungen.

5 Organisation

5.1 Verantwortlichkeiten

ANF5.1 Die oberste Leitung muss in Bezug auf das C]ORE®-Managementsystem die Gesamtverantwortung wahrnehmen.

ANF5.2 Die Organisation muss eine Verpflichtung der obersten Leitung erstellen, fortschreiben und veröffentlichen. Die Oberste Leitung muss verpflichtet sein:

1. die Rechenschaftspflicht für die Wirksamkeit des C]ORE®-Managementsystems zu übernehmen;
2. eine Resilienz-Leitlinie und Ziele für das C]ORE®-Managementsystem festzulegen, die mit dem Kontext und der strategischen Ausrichtung der Organisation vereinbar sind;
3. die Anforderungen des C]ORE®-Managementsystems in die Prozesse der Organisation zu integrieren;
4. die Anwendung eines risikobasierten Vorgehens und resilienzfördernden Handelns zu stärken;
5. die erforderlichen Ressourcen für das C]ORE®-Managementsystem bereitzustellen;
6. die Wichtigkeit und die Bedeutung des C]ORE®-Managementsystem zu vermitteln;
7. die kontinuierliche Verbesserung des C]ORE®-Managementsystems zu fördern;
8. die Führungskräfte anzuleiten ihre Führungsrolle in den jeweiligen Verantwortungsbereichen deutlich zu machen.

> *Hinweis #KRITISDACHG: Für Betreiber kritischer Anlagen ist die Umsetzung der Resilienzmaßnahmen Leitungsaufgabe. Die Geschäftsleitung muss geeignete Organisationsmaßnahmen treffen, damit die Maßnahmen nach § 13 KRITIS-DachG umgesetzt werden (§ 21 Absatz 1 KRITIS-DachG).*

5.2 Beauftragte für organisationale Resilienz

ANF5.3 Die Organisation muss über mindestens eine beauftragte Person für organisationale Resilienz verfügen, die mit ausreichenden Ressourcen ausgestattet ist.

ANF5.4 Die beauftragte Person für organisationale Resilienz muss die organisationale Resilienz in der Organisation fördern und das C]ORE®-Managementsystem mitsteuern und koordinieren.

ANF5.5 Die beauftragte Person für organisationale Resilienz muss regelmäßig und anlassbezogen direkt an die oberste Leitung und wichtige Gremien innerhalb der Organisation (z. B. Mitarbeitervertretung) berichten.

5.3 Weitere Rollen, Verantwortlichkeiten und Befugnisse

ANF5.6 Die Organisation muss die Personen bestimmen und bereitstellen, die für die wirksame Umsetzung ihres C]ORE®-Managementsystems und für das Betreiben und Steuern der Prozesse notwendig sind. Die Organisation muss diesen Personen relevante Rollen zuweisen.

ANF5.7 Die oberste Leitung muss sicherstellen, dass die weiteren Verantwortlichkeiten und Befugnisse für relevante Rollen des C]ORE®-Managementsystems innerhalb der gesamten Organisation zugewiesen, bekannt gemacht und verstanden werden.

ANF5.8 Die Organisation muss die interne und externe Kommunikation, die in Bezug auf das C]ORE®-Managementsystem relevant ist, bestimmen. Sie muss bestimmen, wer mit wem worüber wann wie kommuniziert.

5.4 Ressourcen für das C]ORE®-Managementsystem

ANF5.9 Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die fortlaufende Verbesserung des C]ORE®-Managementsystems sowie die resilienzfördernden Maßnahmen bestimmen und bereitstellen.

ANF5.10 Die Organisation muss für Personen, die relevante Rollen innerhalb des C]ORE®-Managementsystems wahrnehmen, die erforderliche Kompetenz bestimmen. Sie muss sicherstellen, dass die Personen auf Grundlage von angemessener Ausbildung, Schulung oder Erfahrung kompetent sind. Sie muss die Kompetenzen entwickeln, aufrechterhalten und fortlaufend überwachen. Sie muss angemessene Nachweise über die Kompetenz aufbewahren.

ANF5.11 Die Organisation muss das Bewusstsein für die Bedeutung und die Wichtigkeit des C]ORE®-Managementsystems innerhalb der Organisation sowie des äußeren Ökosystems fördern.

ANF5.12 Die Organisation muss regelmäßig innerhalb des inneren und äußeren Ökosystems die Notwendigkeiten und Möglichkeiten der Stärkung der Resilienz kommunizieren.

> *Anmerkung: Die Kommunikation sollte sowohl an Organisationen innerhalb der Lieferkette als auch an Behörden und Verbände gerichtet sein.*

5.5 Dokumentation

ANF5.13 Die Organisation muss dokumentierte Informationen in einem Umfang erstellen, aktualisieren, aufrechterhalten und aufbewahren, wie er

1. von diesem C]A-Standard vorgegeben ist und
2. von der Organisation als notwendig für die Wirksamkeit des C]ORE®-Managementsystems bestimmt wurde.

ANF5.14 Die Organisation muss sicherstellen, dass dokumentierte Information in Übereinstimmung mit dokumentierten Vorgaben

1. erstellt wird (inklusive angemessener Kennzeichnung im Hinblick auf Kennzeichnung und Beschreibung, z. B. Titel, Datum, Autor oder Referenznummer),
2. auf Angemessenheit und Eignung zu überprüft wird,
3. genehmigt wird,
4. angemessen gegen unbefugte Offenlegung geschützt und
5. verfügbar ist, wo und wenn sie benötigt wird.

ANF5.15 Die Organisation muss festlegen, wie

1. Verteilung, Zugriff, Auffindung und Verwendung erfolgen,
2. Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit erfolgen,
3. Änderungen überwacht werden,
4. Aufbewahrung inklusive Aufbewahrungsdauer und Außerkraftsetzung sichergestellt sind.

6 Resilienz-Leitlinie

ANF6.1 Die Organisation muss eine dokumentierte Resilienz-Leitlinie festlegen, umsetzen und aufrechterhalten.

ANF6.2 Die Leitlinie muss

1. strategische Grundsätze des C]ORE®-Managementsystems definieren,
2. konkrete, realistische und messbare Ziele in Bezug auf die Dauer der Aufrechterhaltung der Betriebsfähigkeit in widrigen Situationen, die Dauer der Wiederherstellung sowie den Rahmen für weitere Ziele definiere,
3. die Schadensszenarien benennen, die der Resilienz-Planung zugrunde liegen,
4. eine Verpflichtung zur fortlaufenden Verbesserung beinhalten.

ANF6.3 Die Leitlinie muss innerhalb der Organisation sowie des äußeren Ökosystems bekanntgemacht werden. Für interessierte Parteien muss die Leitlinie verfügbar gemacht werden, sofern dies angemessen ist.

7 Risikomanagement

ANF7.1 Die Organisation muss über ein dokumentiertes, systematisches Vorgehen für ein Risikomanagement verfügen. Sie muss die Häufigkeit der Analyse, involvierte Rollen, den Ablauf und die Berichterstattung festlegen. Hierbei muss sie die Anforderungen des Anhang A umsetzen. Sofern branchenspezifische Erweiterungen vorhanden sind, müssen diese ebenfalls umgesetzt werden.

ANF7.2 Die Organisation muss staatliche Risikoanalysen und -bewertungen sowie andere vertrauenswürdige Informationsquellen nachweislich berücksichtigen.

ANF7.3 Die Organisation muss Kriterien für die möglichen Folgen eines Eintritts sowie die Wahrscheinlichkeit eines Eintritts festlegen und durch die oberste Leitung freigeben lassen. Die Kriterien müssen derart beschrieben sein, dass die Analysen zu vergleichbaren Ergebnissen führen. Die Kriterien müssen die Wirtschaftsstabilität der Organisation sowie die Auswirkungen auf das äußere Ökosystem berücksichtigen.

ANF7.4 Die Risikoanalysen müssen folgende Szenarien umfassen. Hierbei müssen sektorübergreifende oder grenzüberschreitende Szenarien berücksichtigt werden:

1. naturbedingte,
2. klimatisch bedingte und
3. vom Menschen verursachte Unfälle,
4. Naturkatastrophen,
5. gesundheitliche Notlagen,
6. hybride Bedrohungen,
7. feindliche Bedrohungen, einschließlich terroristischer Straftaten sowie
8. weitere von der Organisation oder von branchenspezifischen Erweiterungen als relevant eingestufte Bedrohungen.

> *Hinweis #KRITISDACHG: Betreiber kritischer Anlagen müssen Risikoanalysen und Risikobewertungen auf Grundlage nationaler Risikoanalysen, nationaler Risikobewertungen und anderer vertrauenswürdiger Informationsquellen durchführen. Dabei sind insbesondere Risiken für die Verfügbarkeit kritischer Dienstleistungen sowie Abhängigkeiten von und Auswirkungen auf andere Sektoren, Betreiber und Staaten zu berücksichtigen (§ 12 KRITIS-DachG).*

ANF7.5 Die Organisation muss ein Vorgehen zur Akzeptanz von Risiken festlegen und umsetzen. Hierbei muss sie sicherstellen, dass jedes akzeptierte Risiko nachweislich an die oberste Leitung kommuniziert wird.

ANF7.6 Die Organisation muss über einen Prozess zum Umgang mit und zur Umsetzung von Maßnahmen verfügen, die sich aus dem Risikomanagement ergeben.

ANF7.7 Die Organisation muss für alle Risiken Eigentümer bestimmen. Die Verantwortlichkeiten und Befugnisse der Risikoeigentümer müssen dokumentiert und bekannt gemacht sein.

ANF7.8 Die Organisation muss Zeitspannen von maximal vier Jahren definieren, in denen sie Risikobeurteilungen überprüfen will.

ANF7.9 Die Organisation muss bei der Analyse von Risiken die bestehenden Maßnahmen zur Risikominimierung sowie das aktuelle Risikoniveau (Brutto-Risiko) bestimmen und dokumentieren.

ANF7.10 Die Organisation muss anhand eines methodisch einheitlichen Vorgehens die kritischen Prozesse identifizieren. Sie muss Risikobeurteilungen für die kritischen Prozesse durchführen. Wenn die Organisation Prozesse nicht berücksichtigt, muss sie dies ausführlich begründen und aufzeigen, dass diese keine Auswirkungen auf die kritischen Prozesse oder die Wirtschaftsstabilität haben.

> *Anmerkung: Business Impact Analysen auf Grundlage der ISO 22301 oder anderer anerkannter Standards sind geeignet die kritischen Prozesse zu erheben.*

ANF7.11 Die Organisation muss alle von Dritten bereitgestellten Prozesse, Produkte und Dienstleistungen, die für die kritischen Prozesse und die Wirtschaftsstabilität notwendig sind, bestimmen und dokumentieren. Sie muss Risikobeurteilungen für Prozesse, Produkte und Dienstleistungen durchführen. Wenn die Organisation von Dritten bereitgestellte Prozesse, Produkte und Dienstleistungen nicht berücksichtigt, muss sie dies ausführlich begründen und aufzeigen, dass diese keine Auswirkungen auf die kritischen Prozesse oder die Wirtschaftsstabilität haben.

ANF7.12 Die Organisation muss die Abhängigkeiten der von ihr bereitgestellten Prozesse, Produkte oder Dienstleistungen für Dritte bestimmen und dokumentieren. Sie muss Risikobeurteilungen für diese Abhängigkeiten durchführen. Wenn die Organisation von ihr bereitgestellte Prozesse, Produkte oder Dienstleistungen nicht berücksichtigt, muss sie dies ausführlich begründen und aufzeigen, dass diese keine Auswirkungen auf die kritischen Prozesse oder die Wirtschaftsstabilität haben.

ANF7.13 Die Organisation muss für die in der Analyse der Organisationen mit Einfluss auf die Resilienz (4.2) bestimmten Organisationen eine Bewertung der

1. der Ausfallwirkung,
2. die Widerstandsfähigkeit,
3. der Bewältigungsfähigkeit,
4. der Unterstützungsbedürftigkeit,
5. und des Unterstützungspotentials vornehmen.

> Es muss sichergestellt werden, dass für alle Organisationen mit Einfluss auf die Resilienz die Aspekte anhand der Kritikalitätsstufen (ANF7.3) je Zeitspanne (ANF7.8) bewertet werden. Die Analyse muss die tatsächlichen Prozess- und Lieferketten berücksichtigen. Für die Organisationen mit Einfluss auf die Resilienz kann eine Gruppenbildung vorgenommen werden.

ANF7.14 Die Organisation muss berücksichtigen, welche Vorbereitungsmaßnahmen für die Prävention von und die Reaktion auf Schadenereignisse etabliert sind (Widerstandsfähigkeit) und welche Krisenmanagement- und Kontinuitäts- und Kooperationsplanungen umgesetzt sind (Bewältigungsfähigkeit). Sie muss je Szenario bewerten, wie lange die Organisationen mit Einfluss auf die Resilienz funktionsfähig sind.

ANF7.15 Bei der Bewertung müssen Vertreter der Organisationen mit Einfluss auf die Resilienz einbezogen werden. Es muss sichergestellt sein, dass die Organisationen ausreichend repräsentiert werden. Die Einbeziehung kann durch die Berücksichtigung von Dokumentation erfolgen (z. B. Resilienz-Leitlinien und Erklärungen zur Anwendbarkeit).

ANF7.16 Die Organisation muss für ihre eigenen Organisationseinheiten eine Bewertung der

1. der Ausfallwirkung,
2. die Widerstandsfähigkeit,
3. der Bewältigungsfähigkeit,
4. der Unterstützungsbedürftigkeit,
5. und des Unterstützungspotentials vornehmen.

> Es muss sichergestellt werden, dass für alle Organisationseinheiten die Aspekte anhand der Kritikalitätsstufen (ANF7.3) je Zeitspanne (ANF7.8) bewertet werden. Die Analyse muss die tatsächlichen Prozess- und Lieferketten berücksichtigen. Die Organisation muss für die Organisationsprozesse eine Bewertung der Ausfallwirkung vornehmen.

ANF7.17 Bei der Beurteilung der Widerstands- und Bewältigungsfähigkeit müssen die Anforderungen des Anhanges A berücksichtigt werden. Sofern branchenspezifische Erweiterungen vorhanden sind, müssen diese ebenfalls berücksichtigt werden.

ANF7.18 Aus den Ergebnissen der Analyse müssen auf den Kritikalitätsstufen basierende akzeptable Ausfallzeiten abgeleitet und dokumentiert werden.

ANF7.19 Ausgehend vom Brutto-Risiko und den Ergebnissen der Analysen muss die Organisation entscheiden, welche Risikobehandlungsstrategie sie anwenden möchte. Sie muss die hierfür notwendigen Maßnahmen sowie das erwartete Risikoniveau nach Umsetzung der Risikobehandlungsstrategie (Netto-Risiko) bestimmen und dokumentieren. Bei der Auswahl der Risikobehandlungsstrategie muss die Organisation berücksichtigen, ob der Aufwand zur Umsetzung von Maßnahmen im Verhältnis zur Verwirklichung des Risikos angemessen ist. Die Ergebnisse müssen im Resilienz-Plan berücksichtigt werden.

> *Anmerkung: Als Risikobehandlungsstrategien können unter anderem Minimierung, Vermeidung oder Akzeptanz angewendet werden.*

ANF7.20 In einer Erklärung zur Anwendbarkeit muss die Organisation dokumentieren,

1. welche Maßnahmen des Anhanges A sowie branchenspezifischer Erweiterungen erforderlich sind,
2. eine Option zur Begründung für deren Berücksichtigung wählen (bestehende Maßnahme, Ergebnis des Risikomanagements, vertragliche/gesetzliche Anforderung),
3. den Stand der Umsetzung darstellen, und
4. Begründungen für die Nichtberücksichtigung angeben.

ANF7.21 Die Erklärung zur Anwendbarkeit muss die Organisation, auf Nachfrage Behörden oder Organisationen, auf deren Widerstands- und Bewältigungsfähigkeit sie Einfluss hat, bereitstellen. Hierbei muss die Vertraulichkeit gewahrt werden.

8 Krisenmanagement

ANF8.1 Die Organisation muss eine geeignete Aufbau- und Ablauforganisation umsetzen und aufrechterhalten, die eine Entscheidungsfähigkeit im Ereignisfall sicherstellt. Dies umfasst die Steuerung von Maßnahmen zur Reaktion, Aufrechterhaltung, Wiederherstellung und Wiederanlauf. Sie muss die Einbindung der Organisationen mit Einfluss auf die Resilienz ausgehend von ihren Prioritäten sicherstellen.

ANF8.2 Die Rollen und Verantwortlichkeiten innerhalb der Krisenmanagement-Organisation und die Beziehungen zu anderen Organisationen müssen klar beschrieben werden.

ANF8.3 Die Krisenmanagementorganisation muss aus Personal und entsprechenden Stellvertretungen zusammengesetzt sein, die über die erforderliche Verantwortung, Befugnis und Kompetenz verfügen, um ihre festgelegte Funktion auszuüben.

ANF8.4 Die Organisation muss Pläne und Verfahren zur Aufrechterhaltung und zur Wiederherstellung der Funktionsfähigkeit von Organisationseinheiten und -prozessen sowie der Organisationen mit Einfluss auf die Resilienz aufstellen und fortschreiben, die die Ergebnisse des Risikomanagements (7) berücksichtigen.

ANF8.5 Die Organisation muss Planungen für den Wiederanlauf sowie den Zeitraum nach dem Wiederanlauf aufstellen und fortschreiben, die die erhöhten Ressourcenbedarfe aus der Nacharbeit und -erfassung unterbrochener Organisationsprozesse berücksichtigen.

ANF8.6 Die Organisation muss über Verfahren und technische Hilfsmittel zur internen und externen Kommunikation mit krisenmanagementrelevanten Akteuren verfügen.

ANF8.7 Die Organisation muss über Verfahren und technische Hilfsmittel zur Kompensation des Ausfalls von Notrufstrukturen verfügen.

> *Anmerkung: Es sollten definierte Anlaufpunkte definiert, ausgestattet und kommuniziert werden, die zur Kommunikation mit der Bevölkerung dienen und an denen Hilfsangebote zur Verfügung gestellt werden.*

ANF8.8 Die Organisation muss ein Übungs- und Überprüfungsprogramm verwirklichen und aufrechterhalten, um die Wirksamkeit ihrer Krisenmanagementorganisation und Pläne und Verfahren regelmäßig zu validieren.

ANF8.9 Die Organisation muss aus den Übungen und Überprüfungen Änderungen und Verbesserungen ableiten und umsetzen.

9 Resilienz-Plan

ANF9.1 Die Organisation muss aus den Ergebnissen des Risikomanagements (7) geeignete und verhältnismäßige technische, organisatorische und personelle Maßnahmen zur Förderung ihrer organisationalen Resilienz ableiten und in einem Resilienz-Plan zusammenführen.

ANF9.2 Der Resilienz-Plan muss folgende Inhalte umfassen:

1. Maßnahmen zur Verhinderung von Ereignissen,
2. Maßnahmen zum physischen Schutz sensibler Bereiche, Anlagen und anderer Infrastrukturen,
3. Maßnahmen zur Aufrechterhaltung der Funktionsfähigkeit der Organisationsprozesse und -einheiten sowie der Organisationen von kommunaler Bedeutung,
4. Risiko- und Krisenmanagementverfahren unter Berücksichtigung der Organisationsprozesse und -einheiten sowie der Organisationen von kommunaler Bedeutung;
5. Verpflichtung zur Umsetzung und Zeitplanung.

> *Hinweis #KRITISDACHG: Betreiber kritischer Anlagen müssen Maßnahmen zur Gewährleistung ihrer Resilienz in einem Resilienzplan darstellen und anwenden. Der Resilienzplan muss die zugrunde liegenden Erwägungen erkennen lassen, auf die Risikoanalyse und Risikobewertung Bezug nehmen und bei Bedarf sowie nach Durchführung einer Risikoanalyse und Risikobewertung aktualisiert werden (§ 13 KRITIS-DachG).*

ANF9.3 Der Resilienz-Plan muss Ziele für relevante Organisationseinheiten und Prozesse beinhalten, die im Einklang mit der Resilienz-Leitlinie stehen.

ANF9.4 Die Ziele müssen spezifisch, messbar (sofern möglich), ausführbar, realistisch und terminiert sein.

ANF9.5 Die Organisation muss planen,

1. was getan wird,
2. was der Zielzustand ist,
3. welche Ressourcen erforderlich sind,
4. wer verantwortlich ist,
5. wie die Ergebnisse bewertet werden.

ANF9.6 Der Resilienz-Plan muss innerhalb der Organisation freigegeben werden.

10 Betrieb des C]ORE®-Managementsystems

ANF10.1 Die Organisation muss die Prozesse und Maßnahmen zur Erfüllung der Anforderungen dieses Standards planen, verwirklichen und steuern.

ANF10.2 Die Organisation muss Änderungen planen und sicherstellen, dass diese keine negativen Auswirkungen auf das C]ORE®-Managementsystem, die Widerstands-, die Bewältigungsfähigkeit oder die Wirtschaftsstabilität hat.

ANF10.3 Die Organisation muss Organisationen mit Einfluss auf die Resilienz (insbesondere Lieferanten und Dienstleister) steuern und überwachen. Dies schließt die Durchführung von Vor-Ort-Audits ein.

ANF10.4 Die Organisation muss den Resilienz-Plan umsetzen und fortlaufend fortschreiben.

11 Bewertung und Überprüfung

11.1 Messung und Überwachung

ANF11.1 Die Organisation muss den Stand der organisationalen Resilienz anhand von Kennzahlen messen.

ANF11.2 Die Organisation muss, im Einklang mit den Zielen des Resilienz-Planes (ANF9.3), festlegen

1. was,
2. wie (Methoden),
3. wann,
4. wie häufig,
5. durch wen überwacht und gemessen werden muss, sowie
6. wer die Ergebnisse der Überwachungen und Messungen analysieren und bewerten muss.

11.2 Resilienz-Audits

ANF11.3 Die Organisation muss in geplanten Abständen Resilienz-Audits bei sich selbst und bei den Organisationen mit Einfluss auf die Resilienz durchführen, um Informationen darüber zu erhalten, ob das C]ORE®-Managementsystem den eigenen Anforderungen der Organisation und den Anforderungen dieses Standards entspricht.

ANF11.4 Die Organisation muss eine Auditprogrammplanung erstellen, umsetzen und fortschreiben, die sicherstellt, dass alle Anforderungen dieses Standards und des C]ORE®-Managementsystems regelmäßig überprüft werden.

ANF11.5 Die Organisation muss über dokumentierte Verfahren verfügen, die sicherstellen, wie Audits geplant, durchgeführt, ausgewertet und nachbereitet werden. Sie muss sicherstellen, dass die Auditoren kompetent und unparteilich ausgewählt werden.

ANF11.6 Die Organisation muss mittels dokumentierter Verfahren und Vereinbarungen sicherstellen, dass sie ermächtigt wird, Audits bei den Organisationen mit Einfluss auf die Resilienz durchzuführen oder dass die Organisationen mit Einfluss auf die Resilienz selbstständig Audits durchführen. Sie muss regeln, wie die Ergebnisse der Audits berichtet und umgesetzt werden.

ANF11.7 Die Organisation muss dokumentierte Informationen zu den Resilienz-Audits aufbewahren.

> *Hinweis #KRITISDACHG: Für Betreiber kritischer Anlagen können Audits und die zugrunde liegende Dokumentation als Nachweise für die Einhaltung von Resilienzpflichten herangezogen werden. Zuständige Behörden können insbesondere weitere Informationen, geeignete Nachweise, den Resilienzplan, Auditergebnisse und die Auditdokumentation verlangen (§§ 16 und 17 KRITIS-DachG).*

11.3 Resilienz-Bericht

ANF11.8 Die Organisation muss über dokumentierte Verfahren verfügen, die sicherstellen, dass nachweislich eine regelmäßige und anlassbezogene Berichterstattung gegenüber der obersten Leitung erfolgt. Die oberste Leitung muss die Wirksamkeit, Angemessenheit und Eignung des C]ORE®-Managementsystems bewerten.

ANF11.9 Die Berichterstattung gegenüber der Leitung der Organisation muss Folgendes beinhalten:

1. Status von Maßnahmen aus vorherigen Berichten
2. Veränderungen im Ökosystem
3. Informationen zur Organisation des C]ORE®-Managementsystems
4. Änderungen an der Organisation, sofern zutreffend
5. Änderungen an der Resilienz-Leitlinie, sofern zutreffend

6. Stand und Ergebnisse des Risikomanagements
7. Stand des Krisenmanagements einschließlich Stand und Ergebnissen aus Test und Übungen
8. Stand und Ergebnisse des Resilienz-Planes
9. Ergebnisse aus Messungen und Überwachungen (Kennzahlen)
10. Ergebnisse der Resilienz-Audits
11. Möglichkeiten zur Verbesserung

12 Verbesserung

ANF12.1 Die Organisation muss über dokumentierte Verfahren verfügen, die sicherstellen, dass auf neue Risiken, Nichtkonformitäten, Fehler und Störungen reagiert wird und die möglichen Folgen berücksichtigt werden.

ANF12.2 Die Organisation muss sicherstellen, dass Störungen gegenüber Behörden und Organisationen, auf deren Widerstands- und Bewältigungsfähigkeit sie Einfluss hat, unverzüglich gemeldet werden.

> *Hinweis #KRITISDACHG: Betreiber kritischer Anlagen müssen Vorfälle unverzüglich, spätestens 24 Stunden nach Kenntnis, an die gemeinsame Meldestelle nach § 32 Absatz 1 BSIG melden. Bei andauernden Vorfällen ist die Erstmeldung zu aktualisieren; spätestens einen Monat nach Kenntnis ist ein ausführlicher Bericht zu übermitteln (§ 18 KRITIS-DachG).*

ANF12.3 Die Organisation muss die Notwendigkeit von Maßnahmen zur Beseitigung von neuen Risiken, Nichtkonformitäten, Fehlern und Störungen bewerten. Sie muss die Wirksamkeit der Maßnahmen überprüfen. Sie muss dokumentieren, was getan werden muss, wie die Umsetzung überwacht wird, wann die Maßnahme umgesetzt ist und wer für die Umsetzung verantwortlich ist.

ANF12.4 Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit ihres C]ORE®-Managementsystems fortlaufend verbessern.

13 Anhang A (normativ)

Die in diesem Anhang genannten Maßnahmenziele und Maßnahmen gewährleisten ein einheitliches Mindestniveau bei den Anwendern dieses Standards. Er stellt zudem die Anwendbarkeit des C]ORE®-Managementsystems für Betreiber kritischer Anlagen im Sinne KRITIS-Dachgesetz sicher. Branchenspezifische Erweiterungen des Anhangs basieren auf der gleichen Struktur und ergänzen branchenspezifische Auslegungen der hier aufgeführten Maßnahmenziele und Maßnahmen. Anforderungen mit spezifischem Bezug zur Umsetzung des KRITIS-Dachgesetzes sind mit „#KRITISDACHG" gekennzeichnet. Anwender dieses Standards, die nicht als Betreiber kritischer Anlagen gelten, können die Nichtanwendbarkeit dieser Anforderungen erklären. Alle Anforderungen sind grundsätzlich anwendbar, sofern deren Umsetzung verhältnismäßig im Vergleich zur Beeinträchtigung der Funktionsfähigkeit der Organisation steht.

ID	Bezeichnung	Anforderung
Vorfälle verhindern		
Ziel: Das Auftreten von Vorfällen wird verhindert, indem Richtlinien, Verfahren und Sicherheitsmaßnahmen implementiert werden, die sicherstellen, dass Sicherheitsereignisse und -vorfälle sowie Folgen des Klimawandels frühzeitig erkannt werden.		
A.01	**Richtlinie zum Vorfallerkennung**	Eine Richtlinie zur Erkennung von Sicherheitsvorfällen ist definiert und implementiert. Das Vorgehen der Organisation zur Erkennung von Ereignissen und Vorfällen ist definiert. Alle Mitarbeiter, Dienstleister, Lieferanten und Dritte müssen zur Erkennung und Meldung von Ereignissen verpflichtet werden.
A.02	**Intelligence**	Die internen und externen Quellen zur Sammlung von Informationen und Daten sind bestimmt. Informationen werden regelmäßig erhoben, verarbeitet und ausgewertet, um Muster und Zusammenhänge zu erkennen. Die Ergebnisse werden in ein Bedrohungsbild zusammengeführt.
A.02	**Meldewege**	Sicherheitsereignisse weren umgehend über geeignete Kanäle gemeldet, um sie angemessen zu bewerten.
A.03	**Notfall-kommunikation**	Ein effektives Kommunikationssystem ist etabliert und mit Dritten abgestimmt, um auch in widrigen Situationen schnell relevante Informationen an alle beteiligten Parteien weiterzugeben.
A.04	**Zusammenarbeit mit Behörden und Organisationen** *#KRITISDACHG*	Die Zusammenarbeit im Notfall ist mit relevanten Behörden und Organisationen mit Einfluss auf die Resilienz ist definiert, wird umgesetzt und wird geübt.
A.05	**Cybersecurity**	Sicherheitsmaßnahmen, um Cyberangriffe zu verhindern und die Integrität der Infrastruktur zu gewährleisten, sind geplant und umgesetzt.
A.06	**Klimarisikobewertung** *#KRITISDACHG*	Bewertung der potenziellen Auswirkungen des Klimawandels auf die Infrastruktur werden regelmäßig durchgeführt, um gefährdete Bereiche zu identifizieren.
A.07	**Infrastrukturüberprüfung** *#KRITISDACHG*	Die bestehende Infrastruktur, wird regelmäßig bewertet um Schwachstellen zu identifizieren, die aufgrund von Klimawandelphänomenen (z.B. erhöhte Temperaturen, extreme Wetterereignisse) entstehen.
A.08	**Einhaltung gesetzlicher und vertraglicher Vorschriften**	Alle relevanten gesetzlichen, regulatorischen und vertraglichen Resilienz-Anforderungen sind bestimmt, dokumentiert und werden auf dem neuesten Stand gehalten. Das Vorgehen zur Einhaltung dieser Anforderungen ist dokumentiert und umgesetzt.
A.09	**Kontaktstelle zum BBK** *#KRITISDACHG*	Eine Kontaktstelle oder eine Person mit vergleichbarer Aufgabenstellung ist als Ansprechpartner beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) benannt.

ID	Bezeichnung	Anforderung
A.10	**Austausch mit Netzwerkpartnern**	Regelmäßiger Austausch mit anderen Organisationen und dem Branchennetzwerk, um von bewährten Verfahren zu lernen und von deren Erfahrungen zu profitieren, sind etabliert. Das Vorgehen zur Berücksichtigung der Erkenntnisse ist dokumentiert und umgesetzt.

physischen Schutz der Räumlichkeiten

Ziel: Die physische Sicherheit der Räumlichkeiten und Infrastrukturen wird gewährleistet und unbefugte Zutritte werden verhindert.

B.01	**Reaktionszeiten von Rettungs- und Hilfskräften**	Die Reaktionszeiten aller relevanten Hilfs- und Rettungskräfte für widrige Situationen sind bekannt und werden überwacht. Mit Hilfskräften von Dienstleistern sind Reaktionszeiten vereinbart.
B.02	**Sicherheitszonenkonzept**	Zum Schutz von sensiblen Bereichen, sind ist ein Sicherheitszonenkonzept festgelegt und umgesetzt. Es sind mindestens drei Zonen vorhanden: normale Bereiche, Sicherheitsbereiche, Hochsicherheitsbereiche
B.03	**Perimetersicherung**	Zäunen, Sperren und Barrieren, um den Zugang zu Infrastrukturen zu begrenzen, sind konzeptioniert und umgesetzt.
B.04	**Physischer Widerstand**	Die äußere Struktur des Geländes, der Räumlichkeiten und der Gebäude, aus denen die Einrichtungen der Organisation bilden, sind ausgelegt sein, dass sie einen Widerstand gegenüber Eindringversuchen bieten. Die Summe der Widerstandszeiten ist größer als die Reaktionszeiten von Rettungs- und Hilfskräften. Abweichungen werden angemessen berichtet und behandelt.
B.05	**Berücksichtigung des Stands der Technik** *#KRITISDACHG*	Der Widerstand jedes konstruktiven Elementes ist nach EN 356, EN 1627 bis EN 1630 oder gleichwertig durch Sachkundige bewertet.
B.06	**Videoüberwachung**	Videoüberwachungssystemen zur Überwachung der Umgebung und des Perimeters sind geplant und installiert. Die Anforderungen des Datenschutzes sind berücksichtigt.
B.07	**Verwendung von Sicherheitstechnik** *#KRITISDACHG*	Sicherheitstechnik zur frühzeitigen Erkennung von Eindringversuchen sind an den Übergängen der Sicherheitszonen sowie in den Räumen geplant und umgesetzt. Der Stand der Technik nach EN 50131 oder gleichwertig ist berücksichtigt.
B.08	**Verwendung von Brandmeldetechnik**	Brandmeldetechnik wird geplant und genutzt, um den Sachwertschutz und die Verfügbarkeit der Infrastruktur zu gewährleisten. Der Stand der Technik nach EN 16763 oder gleichwertig ist berücksichtigt.
B.09	**Zugangssteuerung**	Schließ- oder Zugangskontrollsysteme werden verwendet, um sicherzustellen, dass nur berechtigtes Personal Zugang hat. Die Zugangsmedien und -rechte werden regelmäßig geprüft. Dies umfasst auch den logischen Zugriff auf Systeme und Anwendungen.
B.10	**Be- und Überwachung durch qualifiziertes Sicherheitspersonal**	Die Infrastruktur wird regelmäßig durch qualifiziertes Sicherheitspersonal begangen, um verdächtiges Verhalten oder Vorfälle zu erkennen. Sicherheitstechnik wird durch qualifiziertes Sicherheitspersonal in angemessen zertifizierten externen oder gleichwertigen innerbetrieblichen Leitstellen überwacht. Es wird im Einzelfall geprüft, ob Qualifikationen über das gesetzliche Niveau hinaus notwendig sind.

Reaktion auf Vorfälle

C.01	**Planungen für widrige Situationen**	Pläne für widrige Situationen sind dokumentiert und werden regelmäßig überprüft.
C.02	**Ausrüstung für widrige Situationen**	Ausrüstung und -materialien zur Aufrechterhaltung der Betriebsfähigkeit in widrigen Situationen und die Wiederherstellung ist bestimmt, beschafft und wird regelmäßig geprüft.

ID	Bezeichnung	Anforderung
C.03	**Notfallkontakte**	Notfallkontakte sind bekannt und werden regelmäßig aktualisiert.
C.04	**Sofortreaktion**	Die sofortige Reaktion auf Vorfälle und widrige Situationen ist dokumentiert, wird innerhalb der Organisation bekannt gemacht und wird regelmäßig geübt.
C.05	**Verantwortlichkeiten**	Die Verantwortlichkeiten für die Reaktion auf Ereignisse, Vorfälle und widrige Situationen sind festgelegt.
C.06	**Beurteilung von widrigen Situationen**	Alle Ereignisse werden beurteilt, und es wird darüber entschieden, wie sie einzustufen sind (z. B. Störung, Vorfall, Krise).
C.07	**Übung mit Rettungskräften und Behörden**	Die Zusammenarbeit mit Rettungskräften und Behörden wird regelmäßig geübt.
C.08	**Zusammenarbeit mit Versicherern**	Die Zusammenarbeit mit Versicherungsunternehmen ist im Notfall geplant, etabliert und wird umgesetzt, um die Deckung für Notfälle zu überprüfen und sicherzustellen.
C.09	**Zusammenarbeit mit Organisationen mit Einfluss auf die Resilienz**	Die Zusammenarbeit mit Organisationen mit Einfluss auf die Resilienz wird geplant, ist umgesetzt und wird regelmäßig geübt.
C.10	**Zusammenarbeit mit dem BBK** *#KRITISDACHG*	Ein dokumentierter Prozess stellt sicher, dass Vorfälle unverzüglich, spätestens 24 Stunden nach Kenntnisnahme, an die gemeinsame Meldestelle nach § 32 BSIG gemeldet werden. Bei andauernden Vorfällen werden Aktualisierungen übermittelt. Spätestens einen Monat nach der Erstmeldung wird ein ausführlicher Bericht übermittelt.

Wiederherstellung

D.01	**Wiederherstellungsplanung**	Das Vorgehen zur Wiederherstellung der Betriebsfähigkeit nach Vor- und Notfällen ist dokumentiert und wird regelmäßig geübt.
D.02	**Notstromversorgung**	Eine angemessene Notstromversorgung ist geplant und umgesetzt, um die Aufrechterhaltung der Betriebsfähigkeit in widrigen Situationen und die Wiederherstellung zu gewährleisten. Die Angemessen- und Funktionsfähigkeit wird regelmäßig geprüft.
D.03	**Redundanzen**	Technische Einrichtungen werden redundant geplant und vorgehalten, um die Verfügbarkeit zu gewährleisten.
D.04	**Backup und Notfallwiederherstellung**	In einer Notfallwiederherstellungsrichtlinie sind regelmäßige Sicherung von Daten, Systemen und Anwendungen ist geplant. Die Richtlinie ist umgesetzt und wird regelmäßig getestet. Die Wiederherstellungstests müssen die die Bestätigung von Prozessverantwortlichen einbeziehen, um die Verwendbarkeit aus deren Sicht zu beurteilen.
D.05	**Multiple-Sourcing-Strategien** *#KRITISDACHG*	Alternativen Lieferanten, Dienstleister und Logistiklösungen sind für kritische Prozesse bestimmt und vertraglich gebunden, um die Geschäftstätigkeit auch bei Störungen in der Lieferkette aufrechtzuerhalten.
D.06	**Ausweichstandorte**	Die Wiederherstellung von Prozessen und Tätigkeiten der Organisation an alternativen Standorten ist geplant, umgesetzt und wird regelmäßig geübt.

Personalsicherheit

E.01	**Klassifikation von Stellen**	Stellen sind anhand ihrer Kritikalität für die Prozesse klassifiziert.
E.02	**Pre-Employment-Screening**	Vor der Einstellung werden alle Mitarbeiter werden, in Abhängigkeit der Klassifikation der Stelle, einem Pre-Employment-Screening unterzogen. Die Überprüfung der Bewerber beinhaltet mindestens Plausibilitätsprüfungen von Identitätsnachweisen, Originalzeugnissen und beruflicher Erfahrung. Behördliche Sicherheitsüberprüfungen werden, wo rechtlich zulässig, in Betracht gezogen.

ID	Bezeichnung	Anforderung
E.03	**Risikobewertung bei laufender Beschäftigung**	Für alle Mitarbeiter werden, in Abhängigkeit von der Klassifikation der Stelle, anhand eines dokumentierten Prozesses Risikobewertungen beim Auftreten von Risikoindikatoren (z. B: Lohnpfändungen, Privatinsolvenz, laufende Strafrechtsverfahren) durchgeführt. Die abgeleiteten Maßnahmen minimieren das Risiko für die Integrität Prozesse.
E.04	**Wechsel von Stelleninhabern**	Bei Änderung der Beschäftigung, werden in Abhängigkeit von der Klassifikation der Stellen, Maßnahmen umgesetzt, die ein gleichwertiges Niveau im Vergleich zur Neueinstellung gewährleisten. Vergebene Rechte und
E.05	**Beendigung und Änderung der Beschäftigung**	Bei jeder Beendigung oder Änderung des Beschäftigungsverhältnisses, ob geplant oder nicht werden die relevanten internen Ansprechpartner unverzüglich informiert. Vergebene Zugangsrechte werden angepasst oder bei Vertragsende deaktiviert (physischer und logischer Zugang).
Sensibilisierung und Kompetenzbildung		
F.01	**Awareness**	Die Awareness aller Mitarbeiter wird durch geeignete Schulungen, Kampagnen und Informationsmaterial gesteigert. Die Wirksamkeit der Maßnahmen wir gemessen und ausgewertet.
F.02	**Schulungen und Übungen**	Schulungen und Übungen für alle Mitarbeiter werden regelmäßig durchgeführt, um die Kenntnisse über die das Managementsystem, die Resilienzmaßnahmen und Notfallverfahren zu vermitteln und die Reaktionsfähigkeit zu trainieren. Die Schulungen beinhalten eine Einweisung in alle relevanten Richtlinien sowie Verhalten bei Vor- und Notfällen.
F.03	**Kompetenz des Beauftragten für organisationale Resilienz**	Der Beauftragte für organisationale Resilienz verfügt über nachgewiesene Kompetenz in Bezug auf organisationale Resilienz sowie KRITIS-Gesetzgebung.

14 Anhang B (informativ)

Dieser Anhang stellt den Aufbau branchenspezifischer Erweiterungen dar, die als branchenspezifische Resilienzstandards im Sinne des KRITIS-DachG gemeinsam mit anderen Branchenverbänden erstellt werden. Dieser Anhang ist für die Erstellung dieser Dokumente verbindlich anzuwenden. Branchenspezifische Erweiterungen erhalten, nach der Reihenfolge der Veröffentlichung, eine eigene Standardziffer (z. B. C]A-Standard C]ORE Branchenerweiterung)

14.1 Struktur und Inhaltsverzeichnis

Branchenspezifische Erweiterungen zu diesem C]A-Standard haben folgende, standardisierte Struktur.

1. Einleitung
2. Anwendungs- und Geltungsbereich

Für welche Branchen gilt der Standard?

3. Änderungshistorie
4. Branchenspezifische Begriffe
5. Branchenspezifische Resilienzziele

> *Mindestens Dauer der Aufrechterhaltung der Betriebsfähigkeit in widrigen Situationen und die Dauer der Wiederherstellung in Stunden*

6. Branchenspezifische Anforderungen an das C]ORE®-Managementsystem

> Anhang A – branchenspezifische Ergänzungen

Die Kapitel beinhalten lediglich branchenspezifische Beschreibungen. Allgemeine Beschreibungen sind zu vermeiden, soweit möglich, ist auf diesen C]A-Standard zu verweisen.

Kapitel ohne branchenspezifische Ergänzungen werden mit dem Satz „Es gelten ausschließlich die allgemeinen Anforderungen des C]A-Standards C]ORE Basis in der jeweils gültigen Fassung."

14.2 Aufbau des Anhang A – branchenspezifische Ergänzungen

Der Anhang A jeder branchenspezifischen Ergänzung enthält alle Anforderungen des Anhang A dieses C]A-Standards. Branchenspezifische Ergänzungen können durch Erweiterungen der Kontrollen oder zusätzliche Kontrollen spezifiziert werden. Zusätzliche Anforderungen werden an die vorhandenen Kapitel angefügt und fortlaufend beziffert. Sie erhalten den Zusatz .BS (Beispiel: A.11.BS).

Die nachstehende Tabelle gibt eine Anleitung für den Aufbau branchenspezifischer Anhänge.

ID	Bezeichnung	Anforderung	Branchenspezifische Ergänzung
Vorfälle verhindern			
A.01	**Richtlinie zum Vorfallerkennung**	Eine Richtlinie zur Erkennung von Sicherheitsvorfällen ist definiert und implementiert. Das Vorgehen der Organisation zur Erkennung von Ereignissen und Vorfällen ist definiert. Alle Mitarbeiter, Dienstleister, Lieferanten und Dritte müssen zur Erkennung und Meldung von Ereignissen verpflichtet werden.	Die Richtlinie beinhaltet den Ausfall von Störfall-Anlagen im Sinne der 12. BImSchV beinhalten.

ID	Bezeichnung	Anforderung	Branchenspezifische Ergänzung
…			
A.11.BS	**Teilnahme an branchenspezifischen Austauschen**	Keine	Die Teilnahme an den regelmäßigen Sitzungen des Crisis Architecture ist geplant und wird umgesetzt.