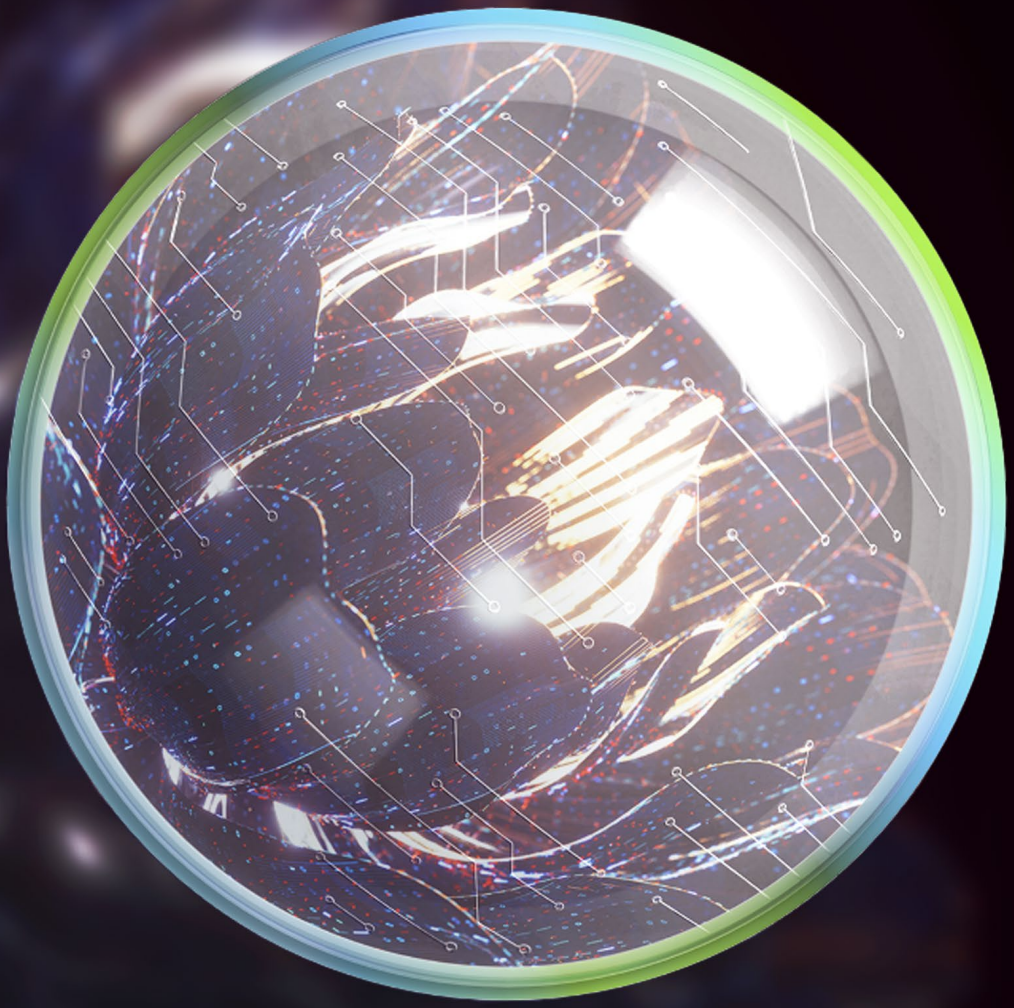
Deloitte.



Schutz kritischer Infrastrukturen
Umsetzung eines modularen Resilienzmanagements

MAKING AN IMPACT THAT MATTERS since 1845

Inhalt

Einleitung

Die Resilienz kritischer Einrichtungen steht nicht zuletzt seit Inkrafttreten der Richtlinie über die Resilienz kritischer Einrichtungen (EU-RCE-Directive | EU 2022/2557) in einem neuen Scheinwerferlicht, das in diesem Umfang erstmalig den Bereich der physischen Sicherheit und Widerstandsfähigkeit beleuchtet.

Auch wenn die sektorenspezifischen KRITIS-Schwellenwerte erst mit Inkrafttreten des KRITIS-Dachgesetzes zur anschließenden Klassifizierung von KRITIS-Betreibern bereitstehen, sind grundsätzliche Entwicklungen für diese bereits absehbar.

Das KRITIS-Dachgesetz wird die nationale Umsetzung der EU-RCE-Direktive darstellen und die kritischen Anlagen entsprechend in folgende Sektoren einteilen (s. Abb. 1).

Kernelemente des zu initiierenden betrieblichen Resilienzmanagements sind:

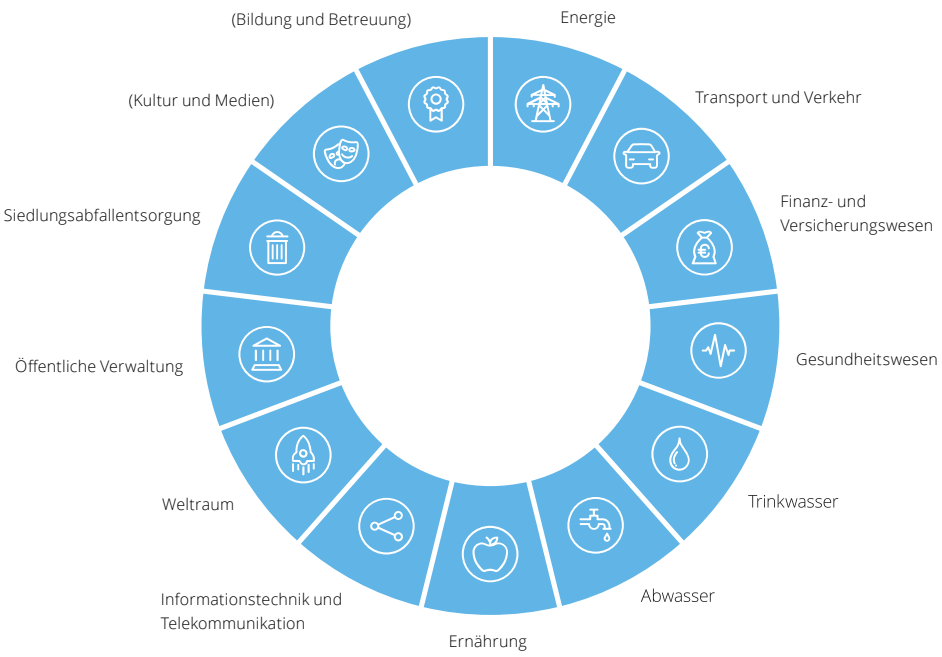
- Einrichtung eines betrieblichen Risiko- und Krisenmanagements
- Durchführung von Risikoanalysen und -bewertungen
- Erstellung von Resilienzplänen
- Umsetzung geeigneter Maßnahmen (technisch, personell, organisatorisch)

Dieses Whitepaper gibt Ihnen einen holistischen Überblick über Anforderungen an die zu initiierende Resilienzplanung sowie ein Spotlight-Update zur grundsätzlichen Planung von Krisenmanagementsystemen entlang des novellierten normativen Standards ISO 22361, welcher unter anderem die Erstellung von spezifischen Krisenmanagementplänen (KMP) im Kontext der Gesamtresilienzstrategie von Unternehmen (Resilienzplanung) vorsieht.

Bereits vorhandene Planungs- und Notfalldokumente z.B. im Rahmen des Business-Continuity-Managements können aufgrund inhaltlicher Synchronisationspotenziale reifegradabhängig (z.B. Reaktiv-, Aufbau- bzw. Standard-BCMS) in die übergeordnete Resilienzplanung integriert werden.

Auch etablierte Prüf- und Planungsmethoden aus dem Bereich anderer Corporate-Governance-Systeme können in den Gesamtkontext der Resilienzplanung gewinnbringend und ressourcenoptimierend integriert werden.

Abb. 1 – Perspektivische KRITIS-Sektoren gemäß KRITIS-Dachgesetz



Betriebliche Resilienzplanung

Business-Continuity Managementsystem
Business-Continuity-Management ist ein Managementsystem, das sicherstellt, dass ein Unternehmen auf unvorhergesehene Ereignisse (Betriebsunterbrechungen) reagieren und seine Geschäftstätigkeit aufrechterhalten bzw. wiederherstellen kann.

Dazu gehört perspektivisch auch die Erstellung von Resilienzplänen, die darauf abzielen, die Auswirkungen von Störfällen auf die Geschäftstätigkeit zu minimieren und deren Wiederherstellung auf Grundlage der definierten Wiederanlaufparameter zu beschleunigen.

Das geplante KRITIS-Dachgesetz soll als KRITIS identifizierte Unternehmen dazu verpflichten, BCM-Maßnahmen im Sinne einer Steigerung der Gesamtresilienz umzusetzen, diese regelmäßig zu überprüfen und in einem zweijährigen Rhythmus (z.B. durch Audits) nachzuweisen.

Konkret beinhaltet dies die Identifizierung von (zeit)kritischen Geschäftsprozessen und die Erstellung von Notfalldokumenten entlang der Phasen Notfallvorsorge und Notfallbewältigung.

Eingebettet in das organisationale Risikomanagement dient das BCM als Teildisziplin somit der Erreichung der nachfolgend dargestellten Zielbilder:

- Aufrechterhaltung der Geschäftstätigkeit (betriebliche Kontinuität) sowie Schutz von Vermögenswerten
- Reputationsmanagement: Eine effektive Reaktion auf kritische Situationen trägt entscheidend zur Wahrung der Reputation bei und erhält das Vertrauen interner sowie externer Stakeholder.
- Kosteneffizienz: Ein Business-Continuity-Management trägt zu einer signifikanten Absenkung der entstehenden Kosten im Ereignisfall bei, da die Ausfallzeit betroffener Geschäftsprozesse und Ressourcen durch vordefinierte Wiederanlaufparameter und die Vor-haltung von operativ-taktischen Strukturen deutlich verringert wird.
- Gesetzliche und regulatorische Anforderungen: In vielen Branchen existieren gesetzliche und regulatorische Anforderungen, die Unternehmen im Sinne des Business-Continuity-Managements erfüllen müssen.
- Wettbewerbsvorteil: Unternehmen, die ein effektives BCM implementiert haben, haben im Vergleich zu ihren Wettbewerbern einen Vorteil, da sie auf Geschäftsunterbrechungen durch vorgeplante Strukturen standardisiert und effizient reagieren können.
- Gewährleistung einer schnellen Wiederherstellung von IT-Systemen und Infrastrukturen

Im Sinne der Resilienzplanung ist ein Business-Continuity-Management für Unternehmen von enormer Bedeutung, um die organisationale Gesamtresilienz sicherzustellen und einem kontinuierlichen Verbesserungsprozess zu unterziehen.

Ein effektives BCM umfasst eine gründliche Analyse zeitkritischer Geschäftsprozesse und Ressourcen, eine in den organisationalen Gesamtkontext eingebettete BCM-Risikobewertung sowie die strukturierte Erstellung von Notfalldokumenten und Prozeduren für den Betrieb der Besonderen Aufbauorganisation (BAO).

Eine umfangreiche institutions- bzw. organisationsspezifische Prüfung des individuell zugrundeliegenden gesetzlichen und/oder regulatorischen Rahmenwerkes („Legal-Framework-Check“) ist unerlässlich, da regulatorische bzw. gesetzliche Anforderungen unter Umständen bereits Prozessanforderungen an ein BCMS definieren, die durch ein Reaktiv-BCMS nicht erfüllt werden können und somit (mind.) ein Aufbau-BCMS erfordern. Branchenspezifische Regulationen ergeben sich bspw. aus den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) bzw. Bankaufsichtliche Anforderungen an die IT (BAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bzw. aus der BSI-KRITIS-Verordnung oder perspektivisch aus dem Regelungsinhalt des KRITIS-Dachgesetzes.

In Abhängigkeit vom von der Organisation definierten Prozessumfang stehen reifegradabhängig drei Modelle von Business-Continuity-Managementsystemen zur Verfügung, um ein betriebliches Kontinuitätsmanagement in der Organisation zu etablieren:

Reaktiv-BCMS
Das Reaktiv-BCMS bietet Organisationen und Institutionen die Möglichkeit, einen schnellen, im Prozessumfang reduzierten Einstieg in die Implementierung eines BCMS zu realisieren, um die zeitkritischsten Geschäftsprozesse initial identifizieren und im Sinne der Ereignisbewältigung absichern zu können.

Die Etablierung eines Reaktiv-BCMS ist somit ideal für Organisationen und Institutionen geeignet, die sich möglichst zeitnah in die Lage versetzen möchten, strukturiert und angemessen unter Zuhilfenahme von kontextsensitiven Handlungsleitfäden auf Ereignisse reagieren zu können.

Hierbei ist es in der Initialphase der Etablierung (Sachstandserhebung) umso wichtiger, eine konsistent holistische Perspektive einzunehmen, um Geschäftsprozesse (Kern-, Teil- und Unterstützungsprozesse) in ihren Interdependenzen erfassen, beurteilen und konzeptionell angemessen berücksichtigen zu können.

Der Reifegrad des Reaktiv-BCMS umfasst somit bewusst (temporär) nur ausgewählte zeitkritische Geschäftsprozesse und Ressourcen einer Institution im Sinne einer initialen Grundabsicherung, die mit vorhandenen Mitteln oder geringfügigen Investitionen realisierbar ist.

Dem gegenüber stehen immer der individuelle Risikoappetit der Institutions- bzw. Organisationsleitung sowie ferner die Reifegradentwicklung im Sinne des kontinuierlichen Verbesserungsprozesses (KVP).

Aufbau-BCMS
Die schrittweise und ressourcenschonende Erweiterung der Resilienzarchitektur mit Bezugnahme auf die zeitkritischen Geschäftsprozesse und Ressourcen einer Institution bzw. Organisation im Sinne des BCMS-Stufenmodells sieht im Reifegrad 2 die Etablierung sowie den wirksamen Betrieb eines Aufbau-BCMS vor.

Das Aufbau-BCMS stellt somit einerseits die modellseitige Aufbaustufe zum Reaktiv-BCMS, andererseits die Ausbaustufe hin zu einem Standard-BCMS (Reifegrad 3) dar.

Als Einstiegsebene im Sinne der BCMS-Reifegrade bietet sich ein Aufbau-BCMS für Institutionen und Organisationen dann an, wenn institutionsseitig bereits erste Erfahrungen im Umgang mit Managementsystemen vorhanden sind und der Wunsch bzw. die Anforderung besteht, personelle und zeitliche Ressourcen qualitativ wie quantitativ an die aufwachsende Struktur des BCMS (Reifegradentwicklung) anzupassen.

Abb. 2 – Eskalationsstufen des Business-Continuity-Managements

Reifegrad	Erläuterung
Störung	• Ungeplante Abweichung vom Regelbetrieb • Bewältigung (Störungsbeseitigung) durch Kräfte der Allgemeinen Aufbauorganisation (AAO) • Keine Aktivierung der Notfallpläne
Notfall	• Nicht tolerierbarer Ausfall (mindestens) eines zeitkritischen Geschäftsprozesses • Aktivierung der Besonderen Aufbauorganisation (BAO) anhand festgelegter Aktivierungs- und Alarmierungsprozesse • Notfallpläne werden aktiviert
Krise	• Nicht tolerierbarer Ausfall (mindestens) eines zeitkritischen Geschäftsprozesses • Aktivierung der Besonderen Aufbauorganisation (BAO) anhand festgelegter Aktivierungs- und Alarmierungsprozesse • Notfallpläne liegen nicht vor, ggf. können bestehende Notfallpläne zur Ereignisbewältigung an das Lagebild adaptiert werden

Dies stellt sicher, dass in der Gesamtbetrachtung Anforderungen an die Wirksamkeit des Systems sowie Qualitätsicherungs- und Awareness-Aspekte institutionsseitig angemessen berücksichtigt werden.

Als methodisches Alleinstellungsmerkmal der Reifegrade Reaktiv- und Aufbau-BCMS wird für die Bemessung grundsätzlich eine Voranalyse durchgeführt, deren Ergebnisse im Rahmen der weiteren Reifegradentwicklung in die Business-Impact-Analyse (BIA) integriert werden können.

Standard-BCMS

Unabhängig vom initial angestrebten BCMS-Reifegrad besteht das strategische Zielbild des Business-Continuity-Managements darin, ein Standard-BCMS zu implementieren und zu betreiben.

Im Rahmen der Reifegradentwicklung des BCMS beträgt der anzunehmende Zeithorizont zwischen den Reifegraden auf Basis unserer Erfahrungen üblicherweise ein Geschäftsjahr.

Durch diesen Zeithorizont-Ansatz der BCMS-Reifegradentwicklung lässt sich dieses oftmals besser in das betriebliche Berichtswesen sowie die geschäftsjährliche Zieldefinition integrieren. Entscheidet sich die Institutionsleitung initial für die Einführung eines Reaktiv- bzw. Aufbau-BCMS (sofern der sektorspezifisch regulatorische Rahmen dies zulässt), so ist diese Entscheidung nachvollziehbar zu begründen und zu dokumentieren.

Als Goldstandard der BCMS-Reifegrade umfasst das Standard-BCMS die Betrachtung aller zeitkritischen Geschäftsprozesse und Ressourcen, inklusive einer vollumfänglichen Analyse von Interdependenzen im Sinne von Prozessabhängigkeiten und diesbezüglichen BC-Kontinuitätsstrategien.

Abb. 3 – Wiederanlaufparameter von Business-Continuity-Managementsystemen (BCMS)

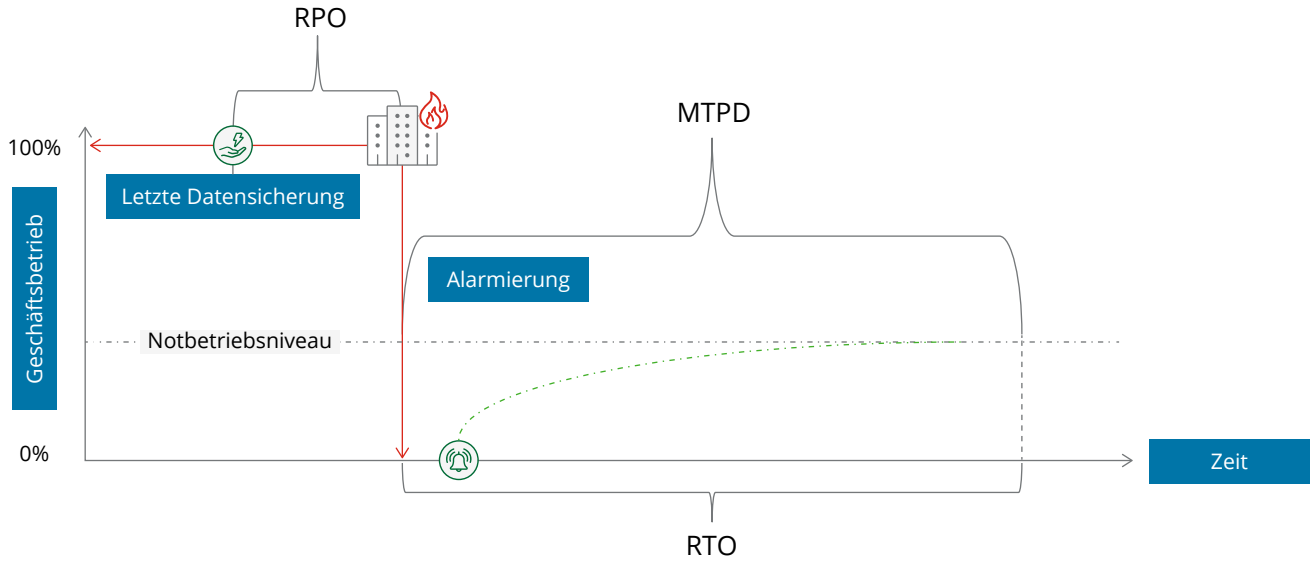


Abb. 4 – Reifegrade von Business-Continuity-Managementsystemen

Reifegrad	Erläuterung
Reaktiv-BCMS	• Besonders geeignet für die zeitnahe Absicherung zeitkritischer Geschäftsprozesse • Durchführung einer Voranalyse gemäß BSI-Standard 200-4 • Idealerweise geeignet für Institutionen und Organisationen ohne Erfahrungen mit Managementsystemen • Keine vollständige Abdeckung aller zeitkritischen Geschäftsprozesse (Risikoappetit der Unternehmensleitung) • Ausgangsbasis für konsistente Reifegradentwicklung hin zum Standard-BCMS • Durch sektorenspezifische gesetzliche und regulatorische Anforderungen teilweise nicht realisierbar
Aufbau-BCMS	• Besonders geeignet für Institutionen und Organisationen, die bereits Erfahrungen mit Managementsystemen besitzen • Methodische Ermittlung von Prozessabhängigkeiten der Institution bzw. Organisation (ab Aufbau-BCMS) • Systematische Erweiterung des Prozessumfangs im Vergleich zum Reaktiv-BCMS • Bei Vorliegen gesetzlicher und/oder regulatorischer Anforderungen ausreichend, wenn alle regulierten Geschäftsprozesse berücksichtigt sind
Standard-BCMS	• Erfassung aller zeitkritischen Geschäftsprozesse • Durchführung einer Business-Impact-Analyse (BIA) • Durchführung einer BCM-Risikoanalyse • Erstellung und Etablierung eines angemessenen Test- und Übungskonzeptes • Vollständige Synchronisation mit anderen Managementsystemen (z.B. ISMS gemäß ISO 27001, BIA) • Das Standard-BCMS bietet der Institution bzw. Organisation den erforderlichen Reifegrad für eine Zertifizierung gemäß ISO-Standard 22301

Hinweis

Nicht jede größere IT-Störung (Major Incident) stellt zugleich einen Notfall im Sinne des Business-Continuity-Managements dar, trotzdem ist ein bidirektionaler Informationsaustausch ohne Zeitverzögerung zwischen den beteiligten Disziplinen (BCM und ITS-CM) über vordefinierte Informations- und Kommunikationswege sicherzustellen, um das Ereignis ggf. in Richtung BCM eskalieren zu können.

Betriebliches Krisenmanagement

Das betriebliche Krisenmanagement dient der strukturierten Reaktion auf außergewöhnliche Ereignisse (Schadenszenarien), die über die Eskalationsstufe des Notfalls hinausgehen und für die im Grundsatz keine Notfalldokumente vorgehalten werden.

Die Bewältigung von Krisen erfolgt durch die Besondere Aufbauorganisation (BAO) des Unternehmens.

Als Krise werden interne oder externe Ereignisse bezeichnet, durch die akute Gefahren für (a) Lebewesen, (b) die Umwelt, (c) Vermögenswerte oder (d) die Reputation des Unternehmens bzw. der Institution drohen.

In Bezug auf die Vorhersehbarkeit werden Krisen in zwei Krisentypen klassifiziert:

1. Ad-hoc-Krise

2. Schleichende Krise

Die **Ad-hoc-Krise** charakterisiert sich dadurch, dass sie plötzlich und ohne Vorwarnung auftritt und eine Bewältigung erfordert.

Sie wird durch installierte Frühwarnsysteme nicht detektiert und kann existenzgefährdendes Wirkungspotenzial besitzen.

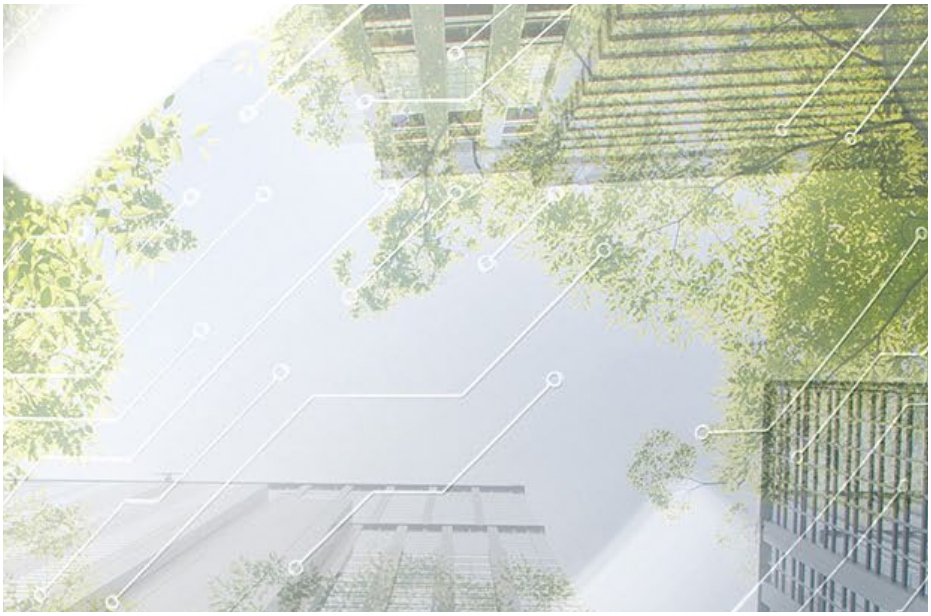
Eine **schleichende Krise** charakterisiert sich dadurch, dass sie zeitlich gesehen langanhaltenden Fortbestand hat und über den Zeitverlauf in ihrem Ausmaß langsam, kontinuierlich anwächst, wie beispielsweise der Verlust von Marktanteilen durch nicht vorhandene Produktinnovationen.

Im führungsorganisatorischen Kontext werden Krisen grundsätzlich durch konzeptionell verankerte Strukturen und Funktionen der Besonderen Aufbauorganisation (BAO) stabsmäßig bewältigt.

Hierbei liegt die Herausforderung häufig in der Gewährleistung der Anschlussfähigkeit der Allgemeinen Aufbauorganisation (AAO) in die Besondere Aufbauorganisation (BAO).

Die in der Organisation vorgehaltenen Notfalldokumente sind somit sinnlogisch so zu gestalten, dass sie einen Informations- und Zeitverlust im Rahmen der Ereignis-Eskalation ausschließen und zugleich einen strukturiert kontextsensitiven Handlungsleitfaden für die Übergabe zwischen den Gremien bieten.

In diesem Kontext sind etwaige Melde- und Berichtspflichten gegenüber Aufsichtsbehörden ebenso zu berücksichtigen (Übergabe der internen Einsatzleitung, Sofort-, Folge- und Schlussmeldungen) wie ggf. aufwachsend zu aktivierende Strukturen (eindeutige Benennung von Aktivierungs- und Eskalationskriterien) für die (politisch) hauptverantwortliche Person (Decision-making Authority).



Basierend auf unseren Projekterfahrungen bietet sich zudem eine Synchronisierung ausgewählter Notfalldokumente mit der übergeordneten Einsatzplanung (EPL) des kommunalen Krisenmanagements bzw. der fachzuständigen Stelle für die nicht-polizeiliche Gefahrenabwehr an, um im Ereignisfall Informations- und Zeitverluste an dieser substanziellen Schnittstelle vermeiden zu können.

Insbesondere empfehlen wir hierzu folgende Maßnahmen:

- Übermittlung relevanter Kontaktdaten interner Schlüsselfunktionen im Ereignisfall an die Leitstelle der nicht-polizeilichen Gefahrenabwehr (Datensätze zentraler Funktionen stehen somit im Einsatzleitsystem der Leitstelle zur Verfügung)
- Synchronisierung ausgewählter Notfalldokumente mit der übergeordneten Einsatzplanung (EPL) der kommunalen nicht-polizeilichen Gefahrenabwehr
- Erstellung einer Dienst- bzw. Organisationsanweisung zur ereignisbezogenen Entsendung von Verbindungspersonen in das kommunale Krisenmanagement

Zentrale Führungsleistungen des Krisenmanagements bestehen somit in der strukturierten Entscheidungsfindung auf Grundlage einer fragilen Informationsbasis einerseits sowie der Erstellung und Aufrechterhaltung eines gemeinsamen Lagebildes anhand der gewonnenen Ergebnisse aus den Arbeits- und Besprechungsphasen des Gremiums andererseits.

Die Vorstellung der Ergebnisse und Erkenntnisse erfolgt dazu in Lagevorträgen zur Unterrichtung (LVU) sowie Lagevorträgen zur Entscheidung (LVE).

Als zentrale Herausforderung ist hier klar die kontinuierliche Aktualisierung des gemeinsamen Lagebildes (Common operational Picture) zwischen der operativ-taktischen und der administrativ-strategischen Ebene herauszustellen, um die Wirksamkeit rückwärtig beschlossener Maßnahmen gewährleisten und ein inaktuelles Lagebild vermeiden zu können.

Auf Grundlage dieser zentralen Herausforderung für Mitglieder der Besonderen Aufbauorganisation (BAO) hat es sich als Good Practice etabliert, einen Übungszyklus von höchstens drei Jahren (Stabsrahmen- bzw. Vollübung) zu etablieren.

Davon unabhängig sind auch unterjährig Alarmierungs- und Funktionstests sowie Planübungen zu initiieren.

Für die betriebliche Gesamtresilienz verfolgt ein effektives Krisenmanagement somit folgende Zielbilder:

- **Vorbereitung:** Ein umfassendes Krisenmanagement sollte regelmäßige Tests, Übungen und Schulungen (Test- und Übungskonzept) beinhalten, um die Mitarbeitenden der Allgemeinen Aufbauorganisation (AAO) sowie auch die Funktionsinhabenden der Besonderen Aufbauorganisation (BAO) auf die Ereignisbewältigung vorzubereiten („in der Krise Köpfe kennen").
- **Schnelle Reaktionszeiten:** Ein angemessenes und wirksames Krisenmanagement sollte dafür sorgen, dass das Unternehmen in der Lage ist, möglichst zeitnah auf Krisenereignisse zu reagieren, ohne signifikante Informations- oder Wissensverluste zu generieren.
- **Kommunikation:** Eine klare und effektive (interne und externe) Notfall- und Krisenkommunikation ist für ein erfolgreiches Krisenmanagement von zentraler Bedeutung, um die Prozess- und Deutungshoheit zu halten.
- **Koordination:** Ein effektives Krisenmanagement verfügt über eine effektive Koordination zwischen allen beteiligten Organisationseinheiten innerhalb des Unternehmens, um es als wissensgetriebene Disziplin zu praktizieren.
- **Lernen aus der Krise:** Ein wirksames Krisenmanagement sollte dafür sorgen, dass das Unternehmen im Sinne einer offenen Feedback- und Fehlerkultur aus bewältigten Ereignissen, Übungen und Tests lernt und seine Verfahren sowie Prozeduren kontinuierlich den Rahmenbedingungen anpasst.

Erstellung von Krisenmanagementplänen

Als Teil der übergeordneten Resilienzplanung haben Organisationen unter anderem ein angemessenes sowie wirksames Krisenmanagementsystem zu betreiben und durch die Bereitstellung entsprechender Ressourcen zu unterhalten.

Als eines der Kernelemente des Krisenmanagementsystems ist die organisationsseitige Erstellung eines Krisenmanagementplans (KMP) vorgesehen, der den normativen Anforderungen der ISO 22361 entspricht.

Im Gegensatz zu der grundsätzlich bekannten szenariobasierten Vorgehensweise aus dem Bereich des Business-Continuity-Managements wird der Krisenmanagementplan (KMP) nicht szenarioabhängig erstellt, wenngleich er Informationen für den Umgang mit spezifischen Krisen (branchenspezifisch vorstellbaren Ereignissen) beinhalten kann und sollte, insbesondere folgende neun Kernelemente:

Rechtliche sowie behördliche Anforderungen

Definierte Aktivierungs- und Eskalationsmechanismen der Krisenreaktion

Funktionsbezogene Zuweisung von Befugnissen und definierten Verantwortungsbereichen

Kontaktinformationen zentraler Ansprechpersonen und Funktionsträger (insbesondere der BAO)

Darstellung der in der Organisation vorhandenen Reaktionsstufen in Abhängigkeit von den definierten Eskalationsstufen

Stabsdienstordnung (Aufbau- und Ablauforganisation des Krisenstabes)

Notfall- und Krisenkommunikationsplan (intern und extern ausgerichtet)

Standard-Vorlagen für die stabsmäßige Ereignisbewältigung (Taktische Arbeitsblätter, Meldevordruck, Lagebericht, kontextsensitive Handlungsleitfäden)

Lage sowie Zutrittsmanagement von Krisenstabsräumen

Darüber hinaus kann der Krisenmanagementplan durch die Festlegung der Strategie sowie weiterer Verfahrenselemente zur Aufbau- und Ablauforganisation des Krisenstabes ergänzt werden.

Organisationsseitig ist dem Krisenmanagementplan folgender Input zuzuführen:

- Methoden zur physischen und virtuellen Visualisierung des Schadenereignisses (Lagebild)
- Kontextsensitive Handlungsleitfäden in Form von Checklisten, taktischen Arbeitsblättern
- Funktions- und Verantwortungsbeschreibungen (Stabsfunktionen, Verbindungspersonen)
- Instrumente und Systeme zur Überwachung und Einbindung sozialer Medien (z.B. Monitoring-Tools bzw. Virtual Operation Support Teams)
- Stakeholder-Analyse
- Templates für die Erstellung des Lageberichts, inkl. Entscheidungsprotokollierung

Krisenmanagementplan (KMP)

Der betriebliche Krisenmanagementplan bildet im Rahmen der übergeordneten Gesamtresilienzstrategie (Resilienzplan) das modulare Grundsatzdokument, das die Anwendung der definierten Prozesse, Verfahren und Ressourcen des Krisenmanagementsystems beschreibt.
Darüber hinaus bildet der KMP reifegradabhängige Schnittstellen, Aktivierungs- und Eskalationskriterien (z.B. Reaktiv-, Aufbau-, Standard-BCMS) ab.
Die Überprüfung des KMP hat gemäß ISO 22361 regelmäßig, in geeigneten Abständen zu erfolgen.

Risikomanagement

Risikomanagement ist ein Managementprozess, welcher zur systematischen Erfassung, Bewertung, Bewältigung und Kommunikation von Geschäftsrisiken im Unternehmen dient.

Grundsätzlich befasst sich das Risikomanagement mit allen Arten an Unternehmensrisiken, die zu einer negativen Planabweichung führen können, wodurch sowohl Betriebsunterbrechungsrisiken als auch Risiken, die sich auf eine kritische Infrastruktur beziehen können, inkludiert sind.

Durch einen gestiegenen Risikoumfang aufgrund externer und interner Einflussfaktoren haben sich unterschiedliche Compliance-Anforderungen sowohl für den Industriesektor als auch den Finanzsektor ergeben:

- Gesetz zur Kontrolle und Transparenz in Unternehmensbereich (KonTraG)
- Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG)
- Gesetz zur Stärkung der Finanzmarktintegrität (FISG)
- Mindestanforderungen an das Risikomanagement von Banken (MaRisk BA)
- EU-Richtlinie 2009/138/EG (Solvency II)

KonTraG

Mit dem KonTraG trat am 1. Mai 1998 ein Artikelgesetz in Kraft, welches durch den Deutschen Bundestag beschlossen wurde, um die Corporate Governance in deutschen Unternehmen zu verbessern. Kern des KonTraG ist die gesetzliche Verpflichtung der Unternehmensleitung zur Einführung eines unternehmensweiten Früherkennungssystems für Risiken (Risikofrüherkennungssystem), damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden. Dies ist entsprechend in § 91 Abs. 2 AktG niedergeschrieben.

In der Gesetzesbegründung (Deutscher Bundestag – Drucksache 13/9712) wird zu § 91 Abs. 2 AktG verdeutlicht, dass es keine neue, sondern eine gesetzliche Hervorhebung der Leitungsaufgaben des Vorstandes nach § 76 AktG ist und bei Pflichtverletzung zur Schadensersatzpflicht führen kann (§ 93 Abs. 2 AktG).

Des Weiteren wird darauf verwiesen, dass keine entsprechenden Regelungen im GmbHG aufgenommen werden und dass § 91 Abs. 2 AktG eine Ausstrahlungswirkung auf Gesellschaften mit beschränkter Haftung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat.

Zu den Fortbestand gefährdenden Entwicklungen gehören im Besonderen die Risiken, welche eine negative Auswirkung auf die Finanz-, Vermögens- und Ertragslage haben können. Darunter sind auch Risiken zu subsumieren, welche einen eindeutigen BCM-Bezug haben und mit diesem Managementsystem abgefedert werden können.

StaRUG

Das StaRuG wurde am 17. Dezember 2020 vom Deutschen Bundestag verabschiedet und trat zum 1. Januar 2021 in Kraft. Mit diesem Gesetz wird erstmals eine verbindliche rechtsformübergreifende Pflicht für die Geschäftsleitung zur Einführung eines Krisenfrüherkennungssystems und -managements geregelt.

Gemäß § 1 Abs. 1 StaRUG „wachen die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können". Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht. Berühren die zu ergreifenden Maßnahmen die Zuständigkeiten anderer Organe, wirken die Geschäftsleiter unverzüglich auf deren Befassung hin.

Ergänzend sind zu dem Krisenfrüherkennungssystem die §§ 101, 102 StaRUG zu sehen, nach denen „Informationen über die Verfügbarkeit der von öffentlichen Stellen bereitgestellten Instrumentarien zur frühzeitigen Identifizierung von Krisen vom Bundesministerium der Justiz und für Verbraucherschutz unter seiner Internetadresse www.bmjv.bund.de bereitgestellt werden" (§ 101 STaRUG) und eine gesetzliche Hinweispflicht für Steuerberater, Steuerbevollmächtigte, Wirtschaftsprüfer, vereidigte Buchprüfer und Rechtsanwälte besteht, wenn bei der Erstellung des

Jahresabschlusses Anhaltspunkte für eine vorliegende Insolvenz offenkundig werden (§ 102 StaRUG).

Damit lehnt sich das StaRUG an die Pflicht des Vorstandes einer Aktiengesellschaft an (§ 91 Abs. 2 AktG) und spricht insbesondere Geschäftsführer von GmbHs an. Jedoch sind auch Geschäftsführer von OHGs, KGs und GbRs, in denen keine natürliche Person haftet, für ein Krisenfrüherkennungssystem verantwortlich.

Da der Gesetzgeber keine Anhaltspunkte dafür liefert, ob und inwieweit die im StaRUG statuierte Pflicht zur Krisenfrüherkennung hinter der im AktG enthaltenen Pflicht zur Risikofrüherkennung zurückbleibt, ist festzuhalten, dass bei Einführung der Maßnahmen nach § 91 Abs. 2 AktG auch die Einführung eines Krisenfrüherkennungssystems nach § 1 Abs. 1 StaRUG erfüllt wird.

FISG

Zum 1. Januar 2022 trat die endgültige Fassung des FISG in Kraft, welches der Stärkung des Vertrauens in den deutschen Finanzmarkt dient. Unter anderem soll dieses Ziel mit der verpflichtenden Einführung eines angemessenen und wirksamen internen Kontrollsystems und Risikomanagementsystems für börsennotierte Aktiengesellschaften (§ 91 Abs. 3 AktG) erreicht werden.

Im Zuge des FISG verpflichtet der neue § 91 Abs. 3 AktG Vorstände börsennotierter Gesellschaften, „darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames IKS und RMS einzurichten". Mit der Formulierung „darüber hinaus" wird auf § 91 Abs. 2 AktG und die dort enthaltene Pflicht zur Implementierung eines Risikofrüherkennungssystems Bezug genommen, für dessen Prüfung WPs bei börsennotierten Aktiengesellschaften gemäß § 317 Abs. 4 HGB im Rahmen der Jahresabschlussprüfung den Prüfungsstandard IDW PS 340 n.F. verwenden. Hieraus sowie aus der Bezugnahme der Regierungsbegründung auf § 107 Abs. 2 S. 3 AktG und auf den DCGK 2022 wird klar, dass § 91 Abs. 3 AktG die Pflicht zur Implementierung eines umfassenden RMS im Sinne des Prüfungsstandards IDW PS 981 vorsieht.

MaRisk BA

Die BaFin hat am 16. August 2021 die finale Fassung der Sechsten Novelle zur Änderung der Mindestanforderungen an das Risikomanagement von Banken veröffentlicht.

Die MaRisk BA geben einen ganzheitlichen Rahmen für das Management der wesentlichen Risiken vor. Dies beruht auf § 25a KWG, welcher die organisatorischen Pflichten von Instituten mit Blick auf das institutsinterne Risikomanagement regelt.

Unter anderem sind die Anforderungen aus den Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) für das Management von Informations- und Kommunikationstechnologie (IKT) und Sicherheitsrisiken (EBA/GL/2019/04) in die aktuelle Fassung der MaRisk BA eingeflossen, soweit diese nicht durch die parallel veröffentlichte Novelle der Bankenaufsichtlichen Anforderungen an die IT (BAIT) adressiert wurden.

Insbesondere wurden aus den IKT-Leitlinien die Anforderungen zum Notfallmanagement übernommen, welche in Abschnitt AT 7.3 MaRisk BA zu finden sind.

Demnach hat das Institut Ziele zum Notfallmanagement zu definieren und aus diesen Zielen einen Notfallmanagementprozess abzuleiten. Für zeitkritische Aktivitäten und Prozesse, welche bei Auswirkungsanalysen identifiziert wurden, sind Risikoanalysen durchzuführen. Des Weiteren ist ein Notfallkonzept für Notfälle in zeitkritischen Aktivitäten und Prozessen aufzustellen. In Notfallkonzepten ist aufzuzeigen, welche möglichen Ersatzlösungen zeitnah zur Verfügung stehen und wie eine Rückkehr zum Normalbetrieb verlaufen sollte.

Mit Abschnitt AT 7.3 zeigen die MaRisk BA eindeutige Verknüpfungen mit dem BCM auf.

Solvency II

Die EU-Richtlinie 2009/138/EG vom 25. November 2009 dient als Basis für das Regelwerk Solvency II betreffend die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit.

Im Einklang mit anderen Finanzdienstleistungsvorschriften wie dem Basel-III-Rahmen für die Bankenaufsicht ist Solvency II ein Regelungsrahmen, der für europäische Versicherungs- und Rückversicherungs-

unternehmen gilt. Die Verordnung soll diesen Unternehmen Anreize bieten, ihre Risikosituation besser zu messen und zu steuern – d.h. niedrigere Solvenzkapitalanforderungen (SKR), niedrigere Preise – und angemessene Risikomanagementsysteme und solide interne Kontrollen einzuführen. Dieser Rahmen ist in drei Säulen gegliedert: Säule I konzentriert sich auf die SKR, Säule II auf die Governance und die Aufsicht und Säule III auf die Offenlegung und die aufsichtliche Berichterstattung.

Mit der zweiten Säule werden die qualitativen Anforderungen an die Governance-Systeme der Erst- und Rückversicherer definiert. Dabei muss jedes Unternehmen die Artikel 41–49 der Solvency-II-Richtlinie (EU-Richtlinie 2009/138/EG) erfüllen.

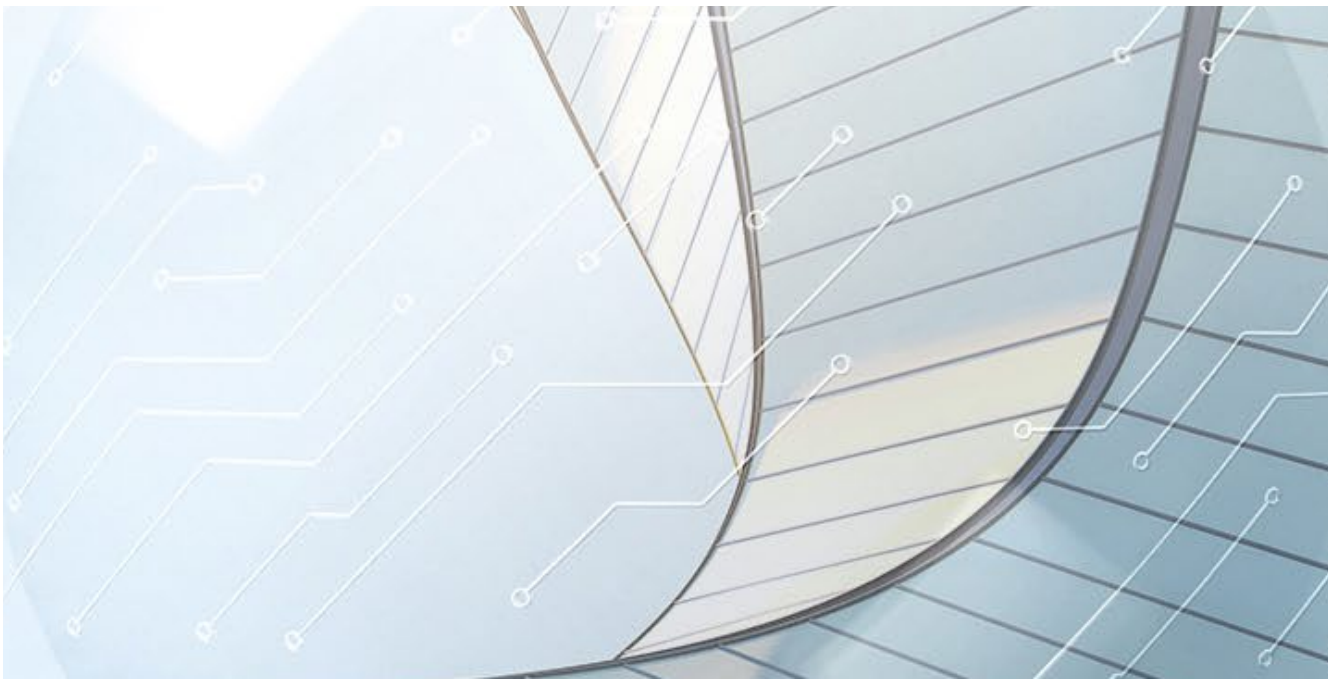
In der nationalen Gesetzgebung sind die Anforderungen in den §§ 23–32 VAG geregelt. Dies betrifft sowohl allgemeine Anforderungen (§ 23 VAG; Art. 41 Solvency II) als auch weitere Anforderungen, welche in den §§ 24, 26, 27, 29–32 VAG (Art. 42, 44–49 Solvency II) definiert sind.

Betrachtet man insbesondere § 23 VAG, so ist in Abs. 4 beschrieben, dass „die Unternehmen angemessene Vorkehrungen, einschließlich der Entwicklung von Notfallplänen, zu treffen haben, um die Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten zu gewährleisten".

In der EU-Richtlinie 2009/138/EG ist in Art. 41 Abs. 4 neben den in § 23 Abs. 4 VAG zu entwickelnden Notfallplänen auch beschrieben, dass „zu diesem Zweck das Unternehmen auf geeignete und verhältnismäßige Systeme, Ressourcen und Verfahren zurückgreift".

Damit schlägt Solvency II eine eindeutige Brücke zur Einrichtung eines BCM.

- § 91 Abs. 2 Aktiengesetz („geeignete Maßnahmen" zur Risikofrühwarnung)
- § 43 Abs. 1 GmbHG (Sorgfalt eines ordentlichen Geschäftsmannes)
- § 317 Abs. 2 Handelsgesetzbuch (HGB) (Vorlage eines Lageberichts durch Leitungsgremien, der die Risiken der künftigen Entwicklung zutreffend darstellt)
- Spezielle Vorgaben Finanzwirtschaft:
  - § 25a Abs. 1 Kreditwesengesetz (KWG) in Verbindung mit AT 7.3 der Mindestanforderungen an das Risikomanagement (MaRisk BA) – „Angemessenes Not-fallmanagement" bzw. „Notfallkonzept"
  - Ferner § 23 Abs. 4 Versicherungsaufsichtsgesetz (VAG) sowie Art. 41 Abs. 4 der Richtlinie 2009/138/EG (Solvency II) – Erstellung von Notfallplänen bei Versicherungen für die „Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten" (vgl. Roselieb et al. 2021: 15)



Glossar

All-Gefahren-Ansatz
Berücksichtigung aller Gefahrenarten (z.B. Naturgefahren, technologische Gefahren etc.) im Rahmen des Risiko- und Krisenmanagements.

Allgemeine Aufbauorganisation
Die ständige Organisationsform einer Institution für die Aufgaben des täglichen Service- bzw. Geschäftsbetriebs.

Besondere Aufbauorganisation
Eine zeitlich begrenzte Organisationsform, um auf außergewöhnliche Situationen angemessen und schnell zu reagieren.

Business-Impact-Analyse (BIA)
Prozess zur Analyse des Einflusses einer Störung auf die Organisation über eine bestimmte Zeit.

Das Ergebnis ist eine Feststellung und Begründung der Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit.

Competent Authority
Zuständige Behörde für die Entgegennahme von Betreibermeldungen im Sinne des zentralen Störungsmonitorings.

Geschäftsfortführungsplan
Geschäftsfortführungspläne dokumentieren auf Geschäftsprozessebene, mit welchen Notfallmaßnahmen eine Institution auf eine Geschäftsunterbrechung reagiert.

ISMS
Informationssicherheitsmanagementsystem

Infrastruktur
Ein Objekt, ein System oder einen Teil davon, das bzw. der für die Erbringung eines wesentlichen Dienstes erforderlich ist.

Kritische Einrichtung
Eine öffentliche oder private Einrichtung einer im Anhang genannten Art, die ein Mitgliedsstaat in Anwendung des Art. 5 der Richtlinie für den Schutz kritischer Einrichtungen (EU 2022/2557) als solche eingestuft hat.

Maximum Tolerable Period of Disruption (MTPD)
Die maximal tolerierbare Ausfallzeit (MTA) gibt auf Geschäftsprozessebene an, wie lange ein Geschäftsprozess maximal ausfallen darf, bevor nicht tolerierbare Auswirkungen für die Institution eintreten.

Minimum Business Continuity Objective (MBCO)
Das Notbetriebsniveau gibt auf Geschäftsprozessebene an, wie leistungsfähig der Notbetrieb sein muss, um den Geschäftsbetrieb sinnvoll gewährleisten zu können.

Plan zur Aufrechterhaltung der Betriebsfähigkeit
Dokumentierte Information, die eine Organisation dabei leitet, auf eine Störung zu reagieren und die Belieferung mit Produkten und Dienstleistungen in Übereinstimmung mit ihren Zielen zur Aufrechterhaltung der Betriebsfähigkeit fortzusetzen, wieder aufzunehmen und wiederherzustellen.

Recovery Point Objective (RPO)
Der maximal tolerierbare Datenverlust gibt an, welcher Datenverlust akzeptiert wird, d.h. wie alt zur Verfügung stehende Datensätze maximal sein dürfen, um diese im Notbetrieb sinnvoll anwenden zu können. Somit ergibt sich aus dem RPO zeitgleich der Parameter des minimal notwendigen Datensicherungszyklus einer Institution.

Recovery Time Actual (RTA)
Die tatsächliche Wiederanlaufzeit bezeichnet den Zeitraum vom Ausfall einer Ressource bis zum Zeitpunkt der Produktivsetzung der BC-Lösung.

Recovery Time Objective (RTO)
Die geforderte Wiederanlaufzeit beschreibt den Zeitraum vom Wiederanlauf (Impact, Detektion, Wiederanlauf) bis zum Erreichen des definierten Notbetriebsniveaus.

Resilienz
Die Fähigkeit, einen Sicherheitsvorfall, der den Betrieb einer kritischen Einrichtung stört oder stören könnte, zu verhindern, abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, aufzufangen, zu bewältigen und die Wiederherstellung zu gewährleisten.

Resilienzplan
Unternehmensbezogenes Grundsatzdokument, das die kumulierten Resilienz-Potenziale einer Organisation darstellt, untereinander referenziert und synchronisiert sowie eine zentrale Ansprechperson benennt.

Risiko
Alle Umstände oder Ereignisse, die potenziell schädliche Auswirkungen auf die Resilienz kritischer Infrastrukturen haben.

Risikobewertung
Eine Methode zur Bestimmung der Art und des Ausmaßes eines Risikos, bei der potenzielle Bedrohungen und Gefahren sowie bestehende Anfälligkeiten, die den Betrieb einer kritischen Einrichtung stören könnten, analysiert und bewertet werden.

Sicherheitsvorfall
Jedes Ereignis, das den Betrieb einer kritischen Einrichtung stört oder stören könnte.

Wesentlicher Dienst
Ein Dienst, der für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten wesentlich ist.

Wiederanlaufplan
Wiederanlaufpläne dokumentieren auf Ressourcenebene, wie ausgefallene Ressourcen in den Notbetrieb (Notbetriebsniveau) überführt werden können.

Wiederherstellungsplan
Wiederherstellungspläne dokumentieren auf Ressourcenebene, welche Maßnahmen zu ergreifen sind, um ausgefallene Ressourcen wieder in den Normalbetrieb zu überführen (Normalbetriebsniveau).

FAQ

Aus welchen Bestandteilen (Modulen) besteht der betriebliche Resilienzplan?

- Überblick über die Gesamtresilienzstrategie des Unternehmens bzw. der Organisation („Tone from the top“)
- Business-Continuity-Managementsystem
  - Reifegradbewertung (Reaktiv-, Aufbau-, Standard-BCMS)
  - Geschäftsfortführungs-, Wiederanlauf- bzw. Wiederherstellungsplanung
  - Notfallhandbuch, inkl. funktions- und szenariobasierten kontextsensitiven Handlungsleitfäden (Checklisten)
  - Allgemeine Aufbauorganisation (AAO) und Besondere Aufbauorganisation (BAO)
  - Test- und Übungskonzept (Funktions- und Alarmierungstests, Stabsrahmenübungen etc.)
  - Taktische Führungs- und Arbeitsmittel zur Lagedarstellung (Common operational Picture)
  - Stabsführungssysteme
  - (Georeferenzierte) Alarmierungs- und Warneinrichtungen
  - Redundanz- und Rückfallebenen
- Supply-Chain-Continuity-Management
- IT-Service-Continuity-Management
- Krisenmanagement
  - Synchronisierung mit übergeordneter Einsatzplanung des kommunalen Krisenmanagements
  - Vordefinierte Entsendung von Verbindungspersonen
  - Melde- und Berichtspflichten gegenüber Aufsichtsbehörden (z.B. Sofort-, Folge- und Schlussmeldungen, D-Meldungsvereinbarungen etc.)
  - Einrichtungen und Prozedere zur Bevölkerungswarnung
- Risikomanagement
  - Risk-Management Manual
  - Risikofrüherkennungssysteme
  - Angemessenheits- und Wirksamkeitsprüfungen
- Security-Management
  - Personelle Sicherheit
  - Travel-Security-Maßnahmen
  - Globales Security-Monitoring
  - Technische Sicherheit (EMA, BMA, Prozessleittechnik)
- Unternehmenskommunikation
  - Notfall- und Krisenkommunikation
  - Social Media Guidelines
  - Virtual Operation Support Teams (VOST)
  - Sicherheitstelefon (intern)
  - Nachbarschaftshotline

Welche Aufgaben haben Beratungsmissionen der EU-Kommission?

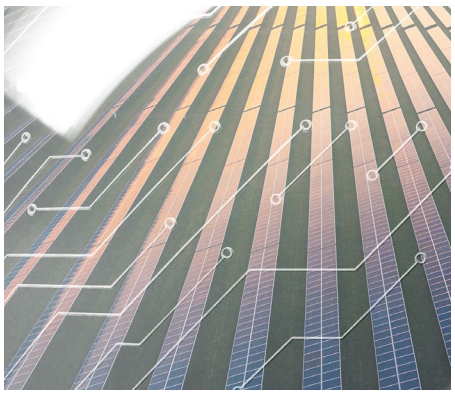
- Beratungsmissionen der EU-Kommission können für kritische Einrichtungen, die für die EU von besonderer Bedeutung sind, durchgeführt werden.
- Kritische Einrichtungen mit besonderer Bedeutung für die EU erbringen für mehr als ein Drittel der EU-Mitgliedsstaaten oder in mehr als einem Drittel der Mitgliedsstaaten wesentliche Dienste.

Welche Aufgaben hat die Gruppe für die Resilienz kritischer Einrichtungen?

- Unterstützung der EU-Kommission und der Mitgliedsstaaten beim Ausbau der Resilienzkapazitäten kritischer Einrichtungen
- Bewertung der nationalen Resilienzstrategien
- Analyse und Beratung zu den Berichten der Beratungsmissionen
- Regelmäßige Tagung mit der durch die NIS-2-Richtlinie eingerichteten Kooperationsgruppe

Innerhalb welches Zeitraums sind kritische Einrichtungen nach deren Einstufung als solche darüber zu informieren?

- Kritische Einrichtungen sind innerhalb eines Monats nach ihrer entsprechenden Einstufung über ihre Verpflichtungen zu informieren.



In welchem Rhythmus ist die Risikoanalyse durch KRITIS-Betreiber durchzuführen?

- Erstmalige Risikobewertung innerhalb von sechs Monaten nach Erhalt des Klassifizierungsbescheids
- Folge-Risikobewertungen mindestens alle vier Jahre bzw. im Bedarfsfall

In welchem Rhythmus ist die staatliche Resilienzstrategie zu aktualisieren?

- Die nationale Resilienzstrategie ist je nach Bedarf, mindestens jedoch alle vier Jahre zu aktualisieren.

Durch welche Behörde wird das zentrale Störungsmonitoring durchgeführt?

- Das zentrale Störungsmonitoring wird durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) durchgeführt.
- Das BBK unterhält bereits das Gemeinsame Melde- und Lagezentrum des Bundes und der Länder (GMLZ).

Welchen Umfang haben Reviews des betrieblichen Resilienzmanagements

- Ist-Stand-Erhebung (initiales Assessment)
- Analyse der Aufbau- und Ablauforganisation des Resilienzmanagements
- Analyse der definierten Wiederanlaufparameter
- Analyse der generierten Notfalldokumente
- Interviews mit Prozessverantwortlichen (z.B. Chief Resilience Officer)
- Identifikation von Punkt- und Linieninfrastrukturen
- Überprüfung der Resilienz-Governance

Welche elf KRITIS-Sektoren existieren?

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Weltraum
- Lebensmittel (Produktion, Verarbeitung, Vertrieb)
- (Kultur und Medien)
- (Bildung und Betreuung)

Für die Sektoren „Kultur und Medien" sowie „Bildung und Betreuung" können Bund und Länder im Rahmen ihrer Zuständigkeiten Resilienzmaßnahmen und ein Monitoring dieser definieren.

Welche Sanktionen drohen bei Nicht-Erfüllung der Anforderungen an kritische Einrichtungen?

- Der explizite Sanktionsumfang ist derzeit noch nicht bekannt.
- Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Wie werden kritische Betreiber identifiziert?

Auf Grundlage der nach § 15 KRITIS-DachG zu erstellenden Rechtsverordnung sind Betreiber kritischer Anlagen (KRITIS) selbstständig dazu verpflichtet, sich anhand der Schwellenwerte zu identifizieren und (digital) zu registrieren.

Für die Registrierung stellen das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine gemeinsame Plattform zur Verfügung.

Welche Unterstützung können kritische Betreiber bei der Umsetzung erwarten?

- Erstellung von Leitfäden und Methoden
- Organisation von Übungen
- Bereitstellung von Schulungen
- Instrumente für den freiwilligen Informationsaustausch

Wie können bestehende Notfallhandbücher in Bezug auf die Resilienzplanung ergänzt werden?

- Bestehende Notfallhandbücher, die im Rahmen des Notfall- bzw. Business-Continuity-Managements für die Funktionen der Besonderen Aufbauorganisation (BAO) angefertigt wurden, können modular zum Resilienzplan ergänzt werden.
- Der Umfang der Notfalldokumente kann funktionsspezifisch angepasst werden.
- Verankerung von klar definierten Aktivierungs-, Eskalations- und Deeskalationsprozessen
- Erstellung von liegenschaftsbezogenen Einsatzplänen (EPL) mit definiertem Szenario-Umfang
- Berücksichtigung von Unternehmens- bzw. Betriebsbereichen in besonderem öffentlichem Interesse (UBI)
- Synchronisierung des modularen Resilienzplans mit der Einsatzplanung des kommunalen Krisenmanagements der nicht-polizeilichen Gefahrenabwehr (Meldevereinbarungen, Entsendung von Verbindungspersonen, objektspezifische Datenpflege im Einsatzleitsystem)
- Notfall- und Krisenkommunikationsplan (inkl. Social Media Guidelines, Virtual Operation Support Team)

Welche Alarmierungsmöglichkeiten für meine Besondere Aufbauorganisation (BAO) habe ich?

- Funktionsgruppen- und Massenalarmierung mit Feedback-Funktion
- Georeferenzierte Alarmierung bzw. Warnung von Funktionsgruppen
- Schnittstellenmanagement zu Incident-Response-Systemen

Ist eine Mehrfach-Managementsystem-Zertifizierung möglich?

- Das betriebliche bzw. organisatorische Resilienzmanagement kann im Rahmen einer Mehrfach-Managementsystem-Zertifizierung ganzheitlich zertifiziert werden.
- Unterhalb der Zertifizierung ist ebenfalls eine Auditierung bzw. ein Review des aktuellen Systemreifegrades möglich.

Welche Anforderungen stellt der DIN-EN-ISO-22361:2021-Entwurf an betriebliche Krisenmanagementsysteme?

- Durchführung einer Wirksamkeitsprüfung
- Erstellung eines Krisenmanagementplans (KMP) im Kontext der Resilienzplanung

Wird es eine Übergangsfrist zur Registrierung und zur Implementierung geforderter Resilienzmaßnahmen gemäß KRITIS-DachG geben?

- Es ist derzeit eine Übergangsfrist bis zum 01.01.2026 vorgesehen.
- Explizit bedeutet dies nach jetzigem Stand, dass folgende Paragraphen des KRITIS-DachG zum 01.01.2026 in Kraft treten:
  - § 6 (Anforderungen an Betreiber kritischer Infrastrukturen)
  - § 7 (Kritische Anlagen von besonderer Bedeutung für Europa)
  - § 8 (Registrierung der kritischen Anlage)
  - § 10 (Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen)
  - § 11 (Resilienzmaßnahmen der Betreiber kritischer Anlagen)
  - § 12 (Meldewesen für Störungen)

Fazit

Ein wirksames Resilienzmanagement bildet als interdisziplinäre Querschnittsdisziplin maßgeblich das Fundament für die Erhöhung der Widerstandsfähigkeit von Unternehmen und Organisationen.

Die Orchestrierung der intern sowie extern beteiligten Teildisziplinen und Managementsysteme setzt profunde Kenntnisse über ihre Methodiken und Bewertungsparameter voraus.

Nicht nur Unternehmen und Organisationen, die vor dem Hintergrund des KRITIS-Dachgesetzes als nationale Umsetzung der EU-RCE-Direktive (Richtlinie zur Stärkung der Resilienz kritischer Einrichtungen) verpflichtend ein Resilienzmanagement vorzuhalten und zu betreiben haben, profitieren von dessen Inhalten, Wirkungs- und Überwachungsbereichen.

Die aufbauorganisatorische Integration des Resilienzmanagements kann nicht allgemeingültig prognostiziert werden, wenngleich die Etablierung eines Chief Resilience Officer (CRO) auf C-Level branchenspezifisch durchaus zu empfehlen ist.

Zur Identifikation der systemischen Kritikalität (u.a. der Zeitkritikalität von Geschäftsprozessen und Ressourcen) sowie des spezifischen Kaskadenpotenzials empfiehlt es sich, bereits im Rahmen der initialen Resilienzplanung eine (KRITIS-)Risikoanalyse durchzuführen.

Die Risikoanalyse betrachtet organisationsspezifisch die Parameter Vulnerabilität und Gefährdung im Sinne einer holistischen Eintritts- und Auswirkungsbewertung im Gesamtkontext aller resilienzrelevanten Management- und Governance-Systeme.

Auf der Risikoanalyse des Resilienzmanagements aufbauend ist es empfehlenswert, eine ergänzende Kritikalitätsanalyse durchzuführen, um das organisationsspezifische Kaskaden- bzw. Domino-Effekt-Potenzial zu ermitteln und daraus gezielt wirksame Maßnahmen und Prozesse zur Minimierung von Betriebsunterbrechungsrisiken zu generieren.

Aufgrund des perspektivisch anzustrebenden Prozessumfangs des Resilienzmanagements und der Vielzahl der reifegradabhängig zu betrachtenden Managementsysteme (z.B. Business-Continuity-Managementsysteme) besteht die klare Empfehlung, dessen Initiierung bereits kurzfristig einzuleiten.

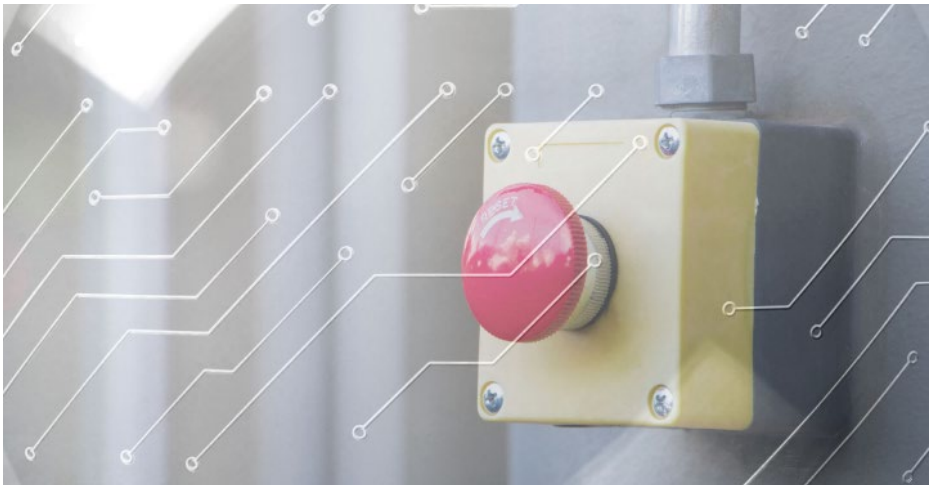
Hinweis

Ganzheitliche Resilienzmanagementsysteme bestehen grundsätzlich aus drei Kernelementen:

Business Continuity Management (BCM), Krisenmanagement und Informationssicherheitsmanagement.

Der Bereich des Informationssicherheitsmanagements gemäß ISO/IEC 27001:2022 wird in einer separaten Publikation separat beleuchtet.

Organisationsspezifisch wird das holistische Resilienzmanagementsystem durch weitere Disziplinen (z.B. Technische Sicherheit, Werkschutz etc.) ergänzt.



Ihre Ansprechpartner

René Scheffler
Partner
Köln
Tel: +49 221 97324 817
rscheffler@deloitte.de

Michael Müller
Partner
Berlin
Tel: +49 30 25468 5225
micmueller@deloitte.de

Deloitte.

Stand 09/2023