Business Continuity Management

Eine Krise kommt selten allein: Wie widerstandsfähig ist Ihr Unternehmen?

Whitepaper BCM & ISO 22301

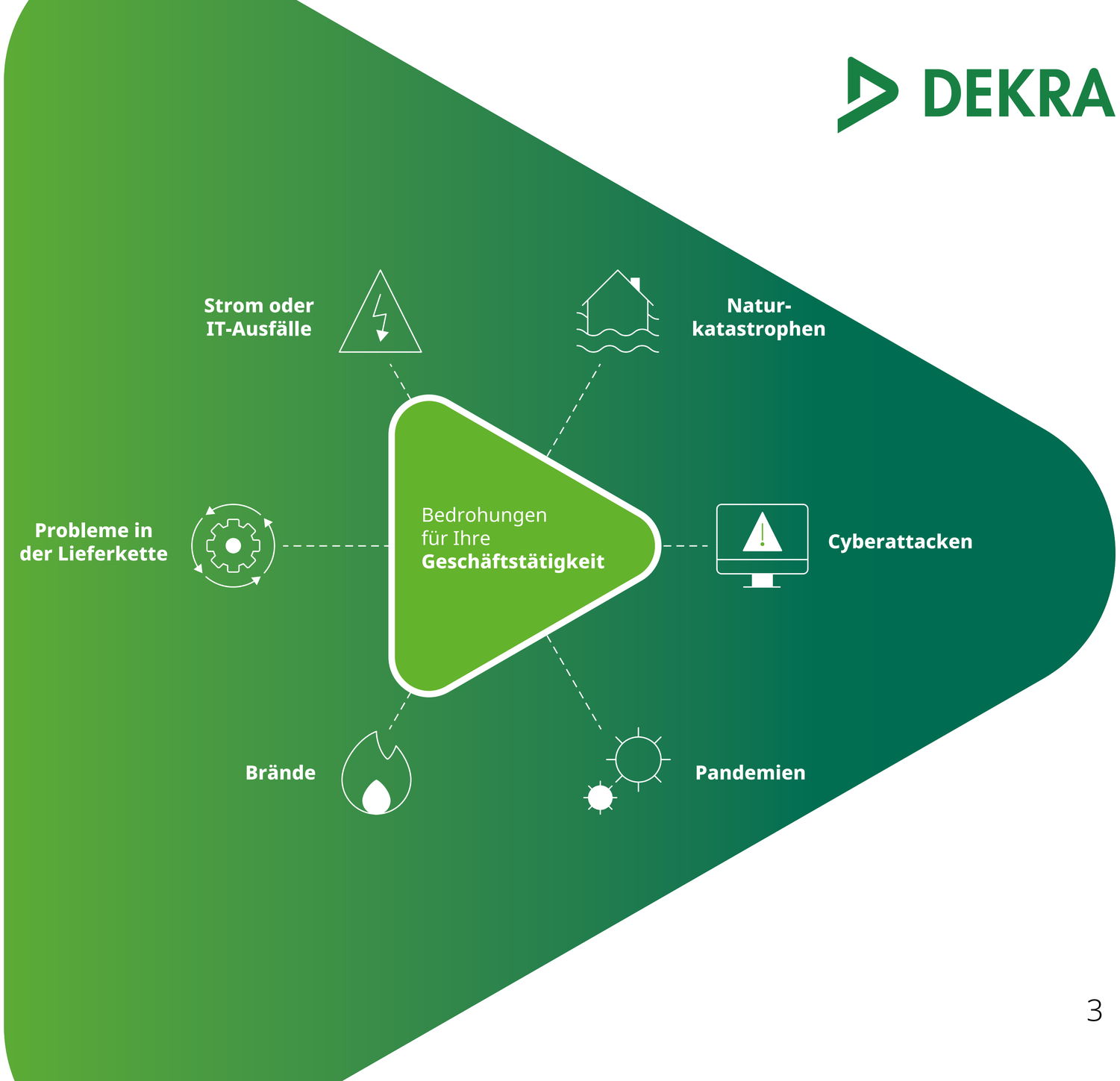
Längst hat sich die Erkenntnis durchgesetzt, dass „business as usual“ aufgrund externer Faktoren wie Fachkräftemangel, volatilen Märkten, Digitalisierung und Globalisierung nicht mehr möglich ist. Auch in Bezug auf unser Risikoverständnis müssen wir uns um eine Anpassung bemühen. Äußere Faktoren wie der Klimawandel oder die politischen Rahmenbedingungen führen dazu, dass wir auch hier „business as usual“ nicht mehr praktizieren können. Treten mehrere kritische Ereignisse gleichzeitig auf, kann dies rasch bis zur existenziellen Betriebskrise eskalieren.

Belastungen für das Kontinuitätsmanagement, wie schon lange nicht

- **Geopolitik:** Etablierte Lieferbeziehungen fallen durch Boykotte oder bewaffnete Konflikte aus. Denken Sie nur an die Halbleiterkrise in der Automobilindustrie im Jahr 2021 zurück.
- **Klima:** Lokale Hitzewellen, Waldbrände mit weiträumigen Luftbelastungen, Stürme, Überschwemmungen oder Erdbeben sind andauernde Gefahren für die Lieferfähigkeit. Zuletzt ereignete sich im Ahrtal ein Jahrhundert-Hochwasser von ungeahntem Ausmaß, welches auch zwei Jahre nach seinem Eintreten noch deutlich spürbar ist.
- **Nachhaltigkeit:** Weltweit restriktivere Regularien für Umweltschutz, Menschenrechte sowie Unternehmensführung (ESG) im Rahmen der LkSG sowie der EU-Corporate Supply Chain Due Diligence Directive (CSDDD), als auch extern verpflichtende sowie intern erklärte Emissionsreduktionen verändern zentrale Prozesse.
- **Digitale Transformation:** Künstliche Intelligenz, Remote-Lösungen sowie digitale Vernetzung transformieren zahlreiche Geschäftsmodelle. Cyber-Gefahren steigen stetig an. So traten laut BSI durchschnittlich zwei Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe pro Monat in 2023 auf.

Bedrohungen für Ihre Geschäftstätigkeit

Die Geschäftsfortführung ist angesichts der zahlreichen Störfaktoren keine Selbstverständlichkeit mehr. Die Folgen von Cyber-Attacken, lokalen Naturereignissen, Ausfällen kritischer Ressourcen und Infrastrukturen sind in den zentralen betrieblichen Prozessen zu berücksichtigen. Folglich sind Organisationen im besonderen Maße herausgefordert, ihre Anpassungs- und Reaktionsfähigkeiten weiterzuentwickeln.



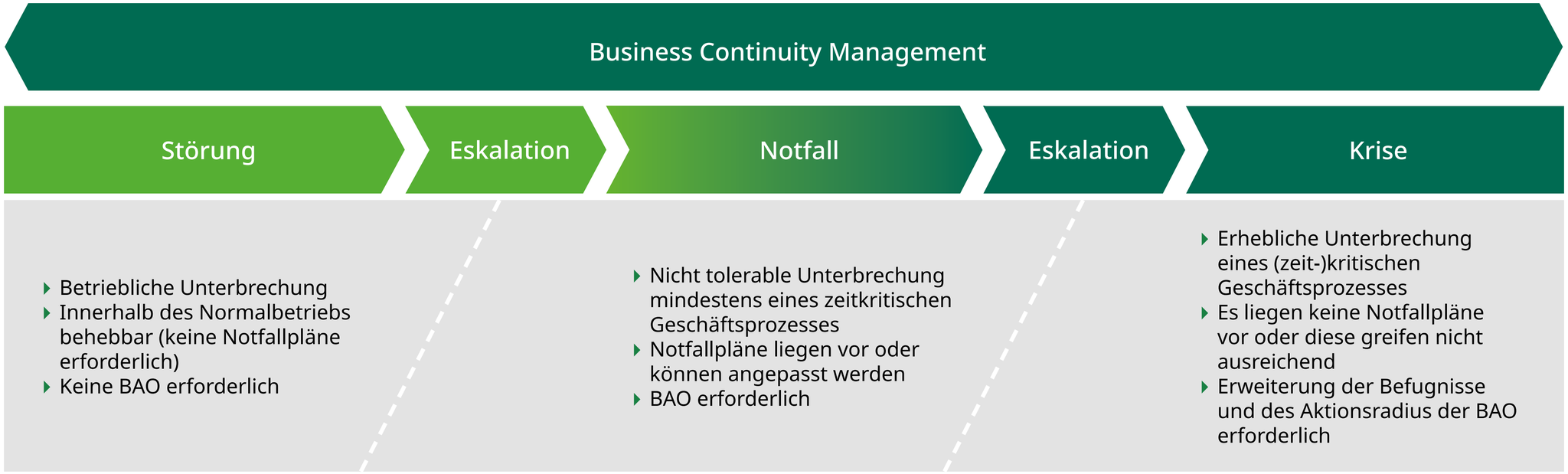


Abb./Quelle: Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-4, 2023

Selbst kleine, bei einzelner Betrachtung eher unbedeutend erscheinende Ereignisse können sich in eng gekoppelten Systemen zum kritischen Schadensereignis hochschaukeln. Eine Störung kann zum Notfall oder einer Krise eskalieren, deren Schwere die Ablauforganisation überfordern kann. Für diese Fällen ist eine zeitlich begrenzte „Besondere Aufbauorganisation (BAO)“ zu bilden und einzusetzen. Unternehmen jeder Betriebsgröße sind daher gut beraten, die Strukturen und Prozesse mit Blick auf die virulenten Risikolagen widerstandsfähiger auszulegen. Ziel des BCMS ist es, so auf kritische Ereignisse zu reagieren, dass die Produktion aufrechtgehalten bzw. die Geschäftsfortführung schnell wieder hergestellt werden können.

ISO 22301: Security and Resilience - Business Continuity Management System

Das Business Continuity Management System (BCMS) auf Grundlage der internationalen Norm ISO 22301 hat sich in der Praxis vielfach bewährt. Mit ihm werden die zentralen funktionalen und operativen Geschäftsprozesse gegen externe und interne Störungen abgesichert. Das Managementsystem richtet sich nicht nur an die IT-Prozesse. Ein wirksames BCMS auf Basis des weltweit anerkannten Standards ISO 22301 als ganzheitlicher Ansatz, betrifft alle Geschäftsbereiche und dient der regelmäßigen Überwachung und Steuerung aller relevanter Faktoren und Umfeldbedingungen, die Auswirkungen auf die Geschäftsfortführung bei Störungen, Notfällen oder krisenhaften Ereignissen haben.

Das BCMS hilft allen Betrieben und Ablauforganisationen jeder Größenordnung, die aktuell relevanten sowie potenzielle Bedrohungen zu erkennen, um darauf aufbauend effektive Gegenmaßnahmen planen und umsetzen zu können. Ist die Betriebsunterbrechung unausweichlich (Cyberattacke, Lieferanten-, Zahlungsausfall, Gebäudeschaden, Boykott etc.), versetzt ein wirksam implementiertes BCMS die Organisation dennoch in die Lage, im tolerablen Zeitrahmen zum Normalbetrieb zurückzukehren. Ausfall- und Wiederherstellungszeiten werden verkürzt und diese Widerstandskraft durch eine Zertifizierung gemäß ISO 22301 gegenüber Kunden, Lieferanten und Kapitalgebern glaubhaft dargelegt.

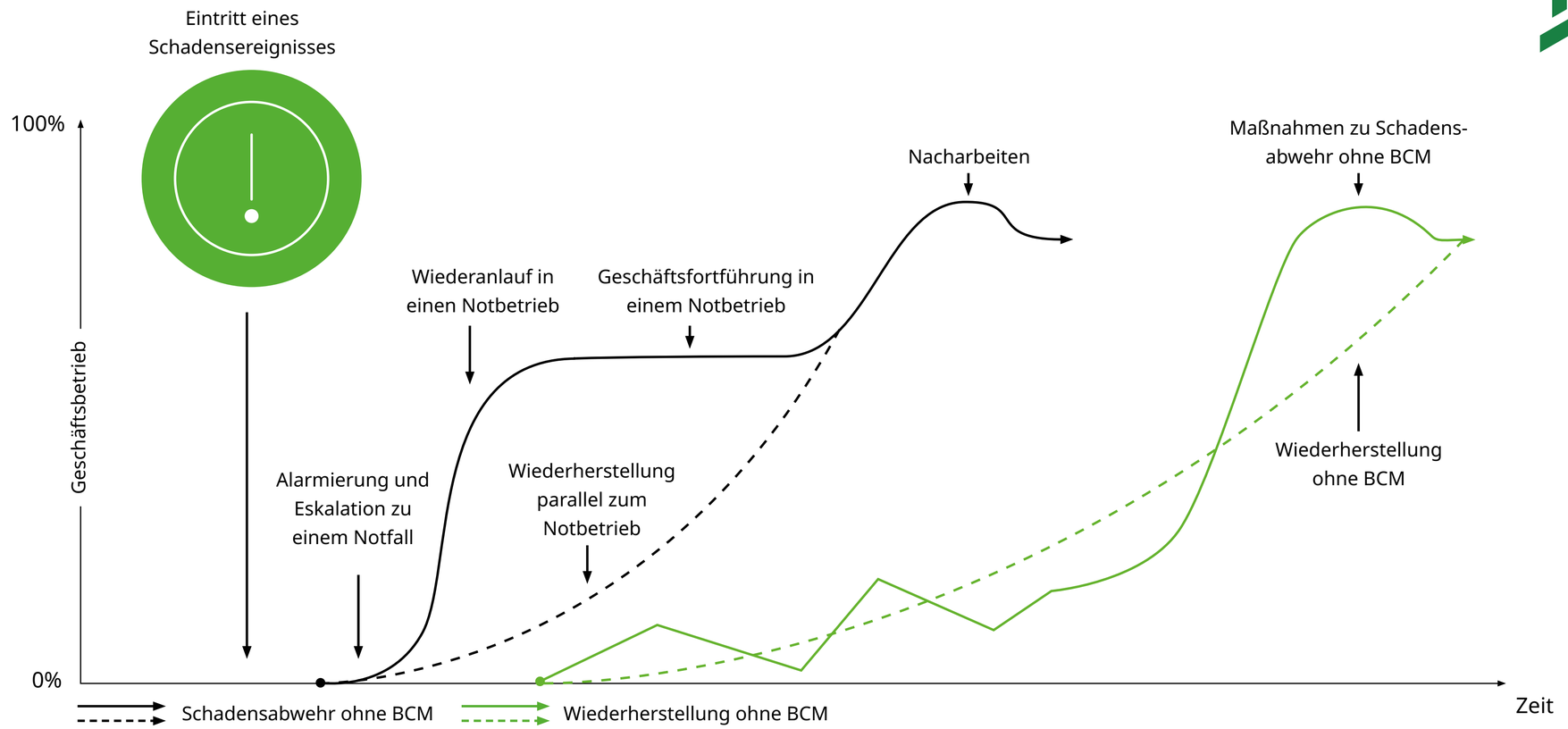


Abb./Quelle: Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-4, 2023

Vorausschauend und proaktiv
Wie jedes normgerechte Managementsystem enthält auch das BCMS das QM-Prinzip der kontinuierlichen Verbesserung. Es eignet sich im besonderen Maße für das Kontinuitätsmanagement und den langfristig angelegten Aufbau von Resilienz. Treten neue Parameter auf, werden die Kernprozesse strukturiert auf etwaige Schwachstellen bewertet und ggf. neu justiert.

Die Folge: Mit jedem Durchlauf des PDCA-Zyklus (Plan, Do, Check, Act) wird der jeweilige Prozess robuster. Mit solch regelmäßigen Soll-Ist-Abgleichen und Evaluierungen kann die Organisation flexibler auf veränderte Umweltbedingungen reagieren, sich beispielsweise auch schneller auf striktere Regulierungen einstellen und frühzeitig auch neue Geschäftschancen erkennen.

ISO 22301: Der Schlüssel zur Absicherung von Geschäftsprozessen

Die Norm ISO 22301[1] unterstützt Unternehmen, damit sie die wichtigsten Geschäftsprozesse gegen eine Störung bis hin zu einem Komplettausfall absichern können. In Kombination mit dem Notfall- und Krisenmanagement ist das BCMS in der Lage, unerwartete Schadensereignisse in den zentralen Anwendungs- und Unternehmensbereichen zu bewältigen. Das BCMS stellt ein belastbares Sicherheitskonzept dar, weil es wie andere Managementsysteme der ISO-Norm auf der Harmonized Struktur des klassischen Qualitätsmanagements (ISO 9001) aufbaut. Bereits die zu erstellenden Basisdokumente legen Grundlagen zur Absicherung wesentlicher betrieblicher Prozesse und dokumentieren Sorgfalt.

1 Die Anforderungen regelt die ISO 22301, während der Leitfaden ISO 22313 die Umsetzung beschreibt. Der BSI-Standard 200-4 als Anleitung zum Aufbau eines BCMS orientiert sich ebenso streng an der ISO 22301.

Die wichtigsten Anforderungen der ISO 22301 umfassen:

Etablierung einer BCM-Politik: Die Organisation muss eine Richtlinie verabschieden, die ihr Bekenntnis zur Business Continuity und die Ziele des BCMS festlegt.

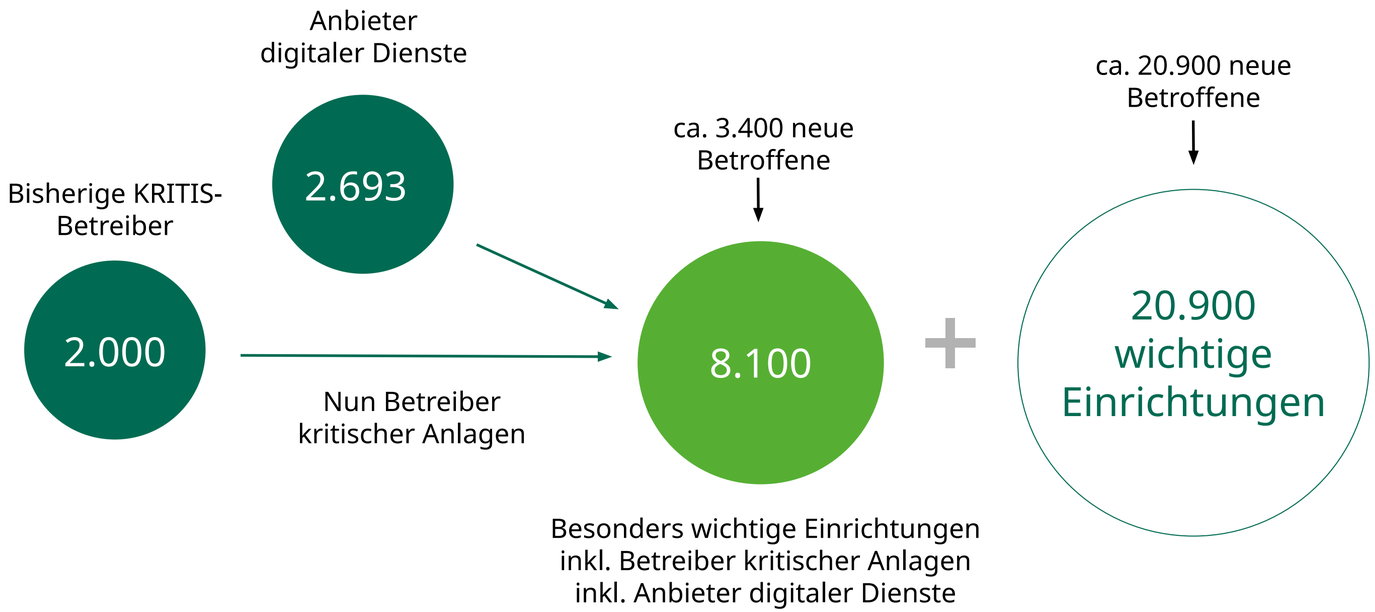
- **Risikobewertung:** Die Organisation muss eine systematische Risikobewertung durchführen, um potenzielle Bedrohungen und deren Auswirkungen auf die Geschäftsprozesse zu identifizieren.
- **Business Impact Analyse:** Die Organisation muss die Auswirkungen von Disruptionen auf die Geschäftsprozesse und die finanziellen Ergebnisse bewerten.
- **Entwicklung von Notfallplänen:** Die Organisation muss Notfallpläne für den Fall von Disruptionen entwickeln, die die wichtigsten Schritte zur Wiederherstellung der Geschäftsprozesse beschreiben.
- **Implementierung und Aufrechterhaltung des BCMS:** Die Organisation muss das BCMS implementieren und aufrechterhalten, einschließlich der Schulung von Mitarbeitern, der Durchführung von Übungen und der Überwachung der Wirksamkeit des Systems.
- **Kontinuierliche Verbesserung:** Die Organisation muss das BCMS kontinuierlich verbessern, um sicherzustellen, dass es den aktuellen Anforderungen und Herausforderungen gerecht wird.

Regulatorische Anforderungen

Die rechtlichen Anforderungen an Business Continuity Management (BCM) können je nach Land, Branche und Art des Unternehmens variieren. Im Allgemeinen gibt es jedoch einige allgemeine Prinzipien und Standards, denen Organisationen folgen können oder müssen. So verankert zum Beispiel der seit Anfang 2021 geltende §1 StaRUG die Pflicht zum Krisenmanagement sowie zur Früherkennung von Krisen. In §1 StaRUG normiert das Gesetz die Haftung der Unternehmensleitung, wenn Krisen erkennbar werden. Somit können Fahrlässigkeit und fehlende Nachweise eines präventiven Krisenmanagements den verantwortlichen Personenkreis im Unternehmen bei Haftungsfall persönlich hart treffen.
Aus dem KonTraG, § 91 Abs. 2 AktG, § 317 Abs. 4 GmbHG und der Sorgfaltspflicht eines ordentlichen Kaufmanns (§347 Abs. 1 HGB) sind verstärkte Anforderungen zu umfassenden Präventionsmaßnahmen zur Sicherung des Geschäftsbetriebs ableitbar.

Rechtsvorschriften und behördliche Anforderungen, nach denen Unternehmen verpflichtet sind, entsprechende Notfallmaßnahmen zu ergreifen bzw. Notfallpläne zu führen, finden sich unter anderem im ArbSchG, dem GmbHG sowie der GefStoffV. So regelt § 10 Abs. 1 des Arbeitsschutzgesetzes (ArbSchG) die Verpflichtung des Arbeitgebers, geeignete „Notfallmaßnahmen“ für außergewöhnliche Situationen zu treffen. Hierzu gehören etwa die Bereitstellung von Notfallplänen und -verfahren einschließlich der Ersten Hilfe, der Brandbekämpfung und der Evakuierung. § 13 GefStoffV geht noch weiter und definiert die Verpflichtung von verfügbaren Notfallplänen und -maßnahmen bei Betriebsstörungen, Unfällen oder Notfällen. Zusätzlich werden ausdrücklich regelmäßige Sicherheitsübungen verlangt.

Betroffenheit in Zahlen



Vor allem in Bezug auf die Nachweispflicht bzgl. physischer Sicherheit und Resilienz ist die EU RCE Verordnung (Resilienz-Baseline für Betreiber kritischer Services in der EU) welche durch das KRITIS-Dachgesetz umgesetzt wird für BCM relevant und tritt ab 10/2024 in Kraft. Der Kreis der betroffenen Unternehmen wird dadurch um weitere 20.900 Betriebe ausgeweitet.

Unternehmen die unter die KRITIS-Verordnung fallen, müssen konkrete Resilienzmaßnahmen in den Bereichen Prävention, physischer Schutz, Reaktion, Wiederherstellung, Personalsicherheit sowie Sensibilisierung nachweisen, sprich BCM im KRITIS-Scope aufnehmen.

Resilienzmaßnahmen

- Frist: 10 Monate
- Physischer Schutz
- Reaktion, Abwehr, Folgenbegrenzung
- Wiederherstellung
- Schulungen, Übungen
- **Konkrete Maßnahmen: §10 (3)**
- Darstellung in Resilienzplan
- Branchenspezifische Resilienzstandards möglich

Prävention

- Notfallvorsorge
- Anpassung an Klimawandel

Psychischer Schutz

- Objektschutz, Zäune, Sperren
- Überwachung der Umgebung
- Detektionsgeräte
- Zugangskontrollen

Reaktion

- Risiko-Management
- Krisen-Management
- Abläufe im Alaramfall

Wiederherstellung

- Aufrechterhaltung des Betriebs (Notstrom etc.)
- Ermittlung alternativer Lieferketten (!)

Personalsicherheit

- Personal-Kategorien
- Zugangsrechte kritische Anlagen etc.
- Zuverlässigkeitsüberprüfungen
- Schulungsanforderungen

Sensibilisierung

- Schulungen
- Informationsmaterial
- Übungen (BCM, Notfallmanagement)

ISO 22301

Diese Aspekte sind bereits in der ISO 22301 enthalten!

BCM und Nachhaltigkeit
BCM hat einen klaren Fokus: die Widerstandsfähigkeit (Alt. Resilienz) von Unternehmen und Organisationen sicherzustellen. Ziel ist es, diese auf potenzielle Störungen vorzubereiten und bei unerwarteten Ereignissen die Geschäftstätigkeit möglichst rasch und kontinuierlich aufrechtzuerhalten, was ein grundlegendes Prinzip in der Norm ist.

Angesichts der wachsenden Auswirkungen des Klimawandels auf Unternehmen spielt BCM auch in Bezug zur Nachhaltigkeit eine wesentliche Rolle und kann dazu beitragen, diese Herausforderungen erfolgreich zu bewältigen.

Durch die Anwendung effektiver BCM-Strategien können Unternehmen potenzielle Risiken bewältigen, die Geschäftskontinuität aufrechterhalten und langfristigen Erfolg sichern. Darüber hinaus fördert BCM ein nachhaltigeres Geschäftsumfeld, indem es Unternehmen dazu anregt, ihre Geschäftsmodelle und -praktiken zu überdenken und verstärkt auf Umweltschutz und Nachhaltigkeit zu setzen.

Ein erfolgreiches BCM trägt dazu bei, die negativen Auswirkungen des Klimawandels auf Unternehmen zu reduzieren und eröffnet gleichzeitig neue Wachstumschancen in einer zunehmend umweltbewussten Welt.

Nachweisbare Maßnahmen zur Steigerung der Resilienz tragen zur Nachhaltigkeit von Geschäftsprozessen bei. Das BCMS unterstützt den Aufbau einer nachhaltigen Organisation, indem die Wirkungsanalyse (Business Impact Analysis) auch ökologische, soziale und ökonomische Risiken sowie ihre Folgen für zentrale Betriebsprozesse berücksichtigen kann.

Ihre Vorteile
auf einen Blick


Absicherung der existenzsichernden **Geschäftstätigkeiten**


Minimierung von **Ausfallzeiten & Wiederaufbau**


Umsetzung der **Compliance-Anforderungen**


Mehr Stabilität der **Arbeitsprozesse**


Risikoeinschätzung aller **Geschäftsbereiche**


International anerkannter **Standard**


Einhaltung **internationaler Standards**


Mehr Engagement seitens der **Führungsebene**

Vorteile und Synergien des BCMS

Zertifizierte Unternehmen zeigen, dass sie effektiv und robust auf unerwartete Bedrohungen reagieren können. Die relevanten Geschäftsbereiche bleiben auch während einer Störung oder Krise funktionsfähig oder können im definierten Zeitrahmen wieder hergestellt werden. Ist das BCMS etabliert, profitieren Unternehmen nicht nur von der gestärkten Widerstandsfähigkeit ihrer zentralen Prozesse, sondern entwickeln darüber hinaus entscheidende Wettbewerbsvorteile hinsichtlich:

Strategie:
- Kommunikation und Umsetzung strategischer Ziele in der Organisation
- Transparenz über aktuelle Risikolagen im Unternehmenskontext
- Gesteigerte Resilienz fördert Reputation und Vertrauen im Marktumfeld/Lieferkette

Finanzen:
- Reduktion finanzieller und rechtlicher Risikopositionen
- Reduktion direkter und indirekter Kosten bei Schadensverläufen
- Absicherung des Unternehmens gegen Umsatzausfälle durch die Betriebsunterbrechungsversicherung
- Verbesserter Zugang zu Kapitalgebern, Versicherungsleistungen, Investoren

Nachhaltigkeit:
- Reduzierte Schadensanfälligkeit zum Schutz für Leib und Leben, Eigentum und Umwelt
- Beachtung der Interessen und regulatorischen Anforderungen aller Stakeholder
- Stärkung von Bewusstsein und Vertrauen der Belegschaft in die Resilienz der Organisation
- Ermittlung, Bewertung wesentlicher Risiken für ESG-Reporting und Compliance
- Absicherung der Lieferketten sowie Einleitung von präventiven Maßnahmen gegen das Ausmaß des Klimawandels

Betrieb:
- Fähigkeiten, zentrale Prozesse bei Störungen aufrechtzuerhalten, effektiv und effizient
- Vorausschauende proaktive Kontrolle und Überwachung von Risiken
- Identifikation und fortlaufende Erhebung potenzieller Schwachstellen

Profitieren Sie bei der Implementierung eines Business Continuity Managementsystem nach ISO 22301 von bestehenden Synergien mit weiteren Management-systemen: ISO 14001 (Umwelt), ISO 3100 (Risk Management, Finance, Supply Chain), ISO 37301 (Compliance), ISO 27001 (Informationssicherheit), ISO 45001 (Arbeits- und Gesundheitsschutz) sowie ISO 50001 (Energie) und mit der CSRD für das Reporting von Nachhaltigkeit.

DEKRA unterstützt Ihr Business Continuity Management System

DEKRA unterstützt mit Experten-Audits den Aufbau einer resilienten Organisation. Unser internationales Netzwerk aus interdisziplinären Branchenexperten und Auditoren steht Ihnen zur Verfügung. Mit der Einführung des BCMS und der Zertifizierung gemäß ISO 22301 ist Ihre Organisation auf eine Vielzahl potenzieller Schadensereignisse vorbereit. Der Zertifizierungsprozess kann die Anforderungen von Kunden, Partnern, Behörden oder Versicherungen nicht nur erfüllen, sondern sogar übertreffen. Das sichert die Geschäftskontinuität und stärkt zusätzlich die Reputation.

Sie möchten mehr über eine Zertifizierung nach ISO 22301 Ihres BCMS erfahren? Kontaktieren Sie uns!

1. Gespräche im Voraus

1.1 Informationsgespräch (optional)
Telefonisches oder persönliches Gespräch mit Ihnen zum Prozessablauf

1.2 Projektgespräch (optional)
Besprechung mit dem Auditor vor Ort bei Ihnen

1.3 Voraudit (optional)
Vorbereitung auf die Zertifizierung inkl. Dokumentenprüfung

2. Zertifizierung*

2.1 Bereitschaftsanalyse
Begutachtung vor Ort und Prüfung der Beschreibung des Managementsystems

2.2 Zertifizierungsaudit
Überprüfung dokumentierter Prozesse des Managementsystems vor Ort

2.3 Nachaudit (optional)
Überprüfen der Korrekturmaßnahmen durch den Auditor

3. Bericht

Dokumentation des Audits inkl. Bewertung des Management- systems

4. Zertifikat und Siegel

Nachweis der erfolgreichen Zertifizierung mit maximal 3 Jahren Laufzeit

5. Erste Überwachung*

Auditierung der Praxisumsetzung des Managementsystems

6. Zweite Überwachung

Wiederholte Auditierung der Praxisumsetzung des Managementsystems

7. Rezertifizierung

Wiederholung der Schritte 2 bis 6 zur Verlängerung für weitere 3 Jahre

*** PDCA-Zyklus**
Fortlaufende Verbesserung durch: Plan, Do, Check, Act.

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de