Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

VEREIN
NETZWERK
LOGISTIK

Business Continuity Management - krisenfeste Versorgungsprozesse

Der KMU-Leitfaden für Business Continuity & Resilienz in den Lieferketten

Impressum

Medieninhaber, Verleger und Herausgeber:
Verein Netzwerk Logistik, Wolfernstrasse 39, 4400 Steyr
Autorinnen und Autoren: VNL GmbH, Prof (FH) DI Dr. Veit Kohnhauser

Fotonachweis:
Cover: midjourne, vnl GmbH

Copyright und Haftung:
Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.

Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundeskanzleramtes und der Autorin/des Autors ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung der Autorin/des Autors dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an office@vnl.at.

Die ReLief4U Leitfäden - Übersicht

Im Rahmen des Projektes "ReLief4U“ wurden mehrere Leitfäden zur Steigerung der Resilienz von Lieferketten für KMUs erarbeitet. Diese bieten einen umfassenden Ansatz in vier aufeinander aufbauenden Teilen:

- ReLief4U - Leitfaden SCRM in KMU: Supply Chain Riskmanagement
- ReLief4U - Leitfaden No 2: Robuste Lieferketten: Der Schlüssel zur Resilienz
- ReLief4U - Leitfaden No 3: Agile Lieferketten gestalten: Ein Praxisleitfaden für KMUs
- ReLief4U - Leitfaden No. 4: Business Continuity Management: Ein Leitfaden für KMUs

Inhaltsverzeichnis

Die ReLief4U Leitfäden - Übersicht 3
Inhaltsverzeichnis 4
Einleitung 6
Krisenfest durch Business Continuity Management (BCM) 6
Bedeutung von BCM für KMU 7
Business Impact Analysis 8
Schritt 1: Identifikation der Geschäftsprozesse 8
Schritt 2: Ermittlung von potenziellen Incidents und Auswirkungen 8
Schritt3: Quantifizieren des Impacts 8
Schritt 4: Bestimmung der Kritikalität der Incidents 9
Schritt 5: Erstellung eines Impact Scores: 9
Schritt 6: Risikobewertung 9
Fallbeispiel - Berechnung Business Impact 10
Schritt 1: Identifikation der betroffenen Geschäftsprozesse 10
Schritt 2: Ermittlung der Auswirkungen pro Geschäftsprozess 11
Schritt 3: Quantifizierung des Impacts 11
Schritt 4: Quantifizierung der indirekten finanziellen Verluste 12
Schritt 5: Gesamtkostenberechnung 12
Schritt 6: Festlegung von Recovery Objectives 13
Schritt 6: Risikobewertung 13
Schritt 7: Maßnahmen und Fazit 13
BCM für Geschäftsprozesse 14
Relevante Standards, Normen und Richtlinien 15
Internationale Standards 15
ISO 22301 Business continuity management systems 15
ISO 22313 - Guidance on the use of ISO 22301 15
ISO 27001 - Informationssicherheit, Cybersicherheit und Datenschutz 15
Nationale Standards & Richtlinien 16
BSI-Standard 200-4: Business Continuity Management (BCM) 16
Österreichisches Informationssicherheitshandbuch 16
Gesetze & Verordnungen 16
Netz- und Informationssystemsicherheitsgesetz 16

Datenschutzgrundverordnung (DSGVO) 16
Weitere relevante Aspekte 16
Versicherungspflichten 16
Vertragliche Verpflichtungen 16
Checkliste zur Umsetzung von BCM in KMU 17
Präventive Maßnahmen 17
Reaktive Maßnahmen 18
Spezifische Maßnahmen für Ihre Geschäftsprozesse 18
Zusätzliche Tipps 19
Auswertung 19
Wichtige Hinweise 19
Nächste Schritte 19
Fazit & Ausblick 20
Abbildungsverzeichnis ..... **Error! Bookmark not defined.**
Literaturverzeichnis ..... **Error! Bookmark not defined.**
Glossar ..... **Error! Bookmark not defined.**

Einleitung

Krisenfest durch Business Continuity Management (BCM)

Business Continuity Management (BCM) ist ein systematischer Ansatz, der Unternehmen dabei hilft, auf unerwartete Ereignisse vorbereitet zu sein und den Geschäftsbetrieb aufrechtzuerhalten oder schnellstmöglich wiederherzustellen. Es geht darum, die **kritischen Geschäftsprozesse** zu identifizieren, die Auswirkungen von Betriebsunterbrechungen zu bewerten und geeignete Maßnahmen zu entwickeln, um diese zu vermeiden oder zu minimieren. Schon kleine Störungen im IT-System oder im der IT-Infrastruktur können für KMU schwerwiegende Folgen haben, wie z.B. finanzielle Verluste, Imageschäden und im schlimmsten Fall sogar die Existenzbedrohung.

Um die Versorgungssicherheit und die operative Geschäftstätigkeit von KMU zu gewährleisten, sollten zumindest folgende Prozesse im BCM berücksichtigt werden:

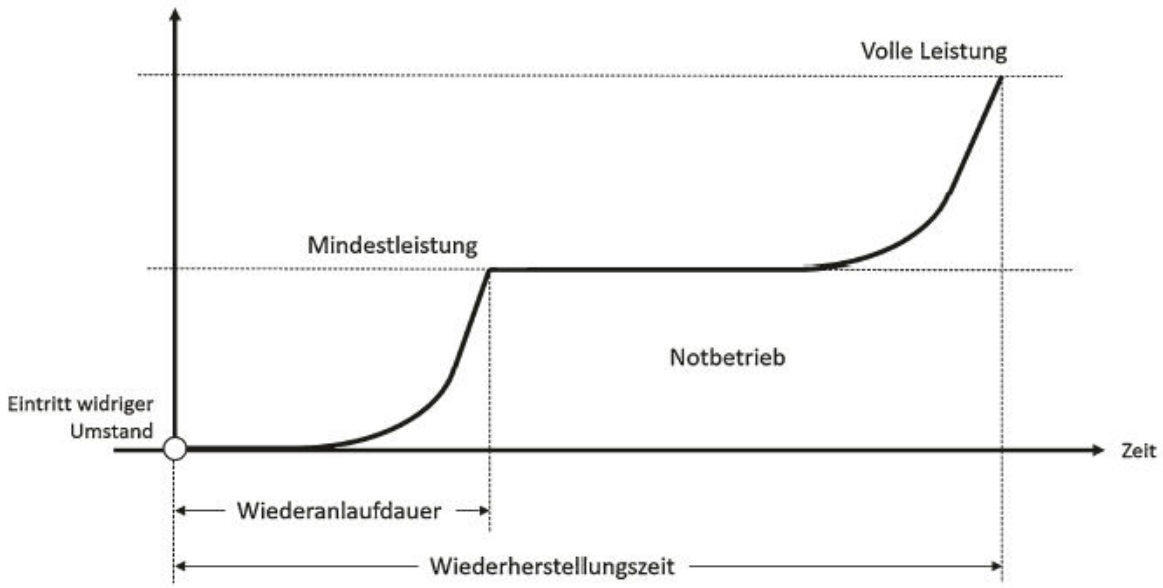
- **Angebotserstellung:** Erstellung eines individuellen Angebots für den Kunden
- **Auftragserfassung:** Erfassen und Prüfen von Kundenaufträgen.
- **Kreditprüfung**: Überprüfung der Zahlungsfähigkeit des Kunden.
- **Lagerverwaltung:** Überprüfung der Verfügbarkeit von Produkten, Reservierung von Lagerbeständen.
- **Beschaffung:** Bestellung von Rohstoffen und Materialien.
- **Auftragsplanung / -steuerung**: Einplanung von Produktionsaufträgen, Bestellungen, Dienstleistungen
- **Qualitätskontrolle**: Prüfung der Produktqualität.
- **Kommissionierung**: Zusammenstellen der bestellten Artikel.
- **Verpackung und Versand**: Verpacken der Ware, Erstellen von Versanddokumenten, Übergabe an den Versanddienstleister.
- **Export- & Zollabwicklung:** Erstellung von Exportdokumenten und die Zollabwicklung.
- **Fakturierung**: Erstellen und Versenden von Rechnungen.
- **Zahlungseingang**: Verbuchung von Zahlungseingängen.
- **Retourenmanagement**: Bearbeitung von Rücksendungen.
- **Kundenkommunikation**: Auskunft über Status und Bearbeitung von Kundenanfragen.
- **After-Sales-Service:** Bearbeitung von Gewährleistungsansprüchen oder die Bereitstellung von technischem Support.

Die genaue Definition der Geschäftsprozesse ist abhängig von der jeweiligen Organisation und ihren spezifischen Anforderungen.

Bedeutung von BCM für KMU

Im Gegensatz zu großen Unternehmen verfügen KMU oft über begrenzte Ressourcen und internes Know-how und können sich längere Ausfallzeiten oder Datenverluste und die damit verbunden Kosten nicht leisten. Daher ist es essenziell, proaktiv Maßnahmen zu ergreifen, um auf potenzielle Risiken wie Cyberangriffe, Stromausfälle oder IT-Probleme vorbereitet zu sein.

1. **Existenzsicherung:** Ein unvorhergesehener Ausfall oder schwerwiegender Cyberangriff kann für KMU existenzbedrohend sein. BCM hilft, solche Risiken zu identifizieren und Strategien zu entwickeln, um den Geschäftsbetrieb aufrechtzuerhalten.
2. **Kundenvertrauen:** Die Fähigkeit, auch in Krisenzeiten zuverlässig zu liefern, stärkt das Vertrauen der Kunden und fördert langfristige Geschäftsbeziehungen.
3. **Gesetzliche Anforderungen und Compliance:** In einigen Branchen sind bestimmte BCM-Maßnahmen gesetzlich vorgeschrieben. Die Einhaltung dieser Vorschriften vermeidet rechtliche Konsequenzen.
4. **Wettbewerbsvorteil:** Unternehmen, die auf Störungen vorbereitet sind, können schneller reagieren und haben einen Vorteil gegenüber Wettbewerbern, die keine BCM-Maßnahmen implementiert haben.



Quelle ergänzen

Business Impact Analysis

Der **Business Impact** bezeichnet die Auswirkungen, die ein bestimmter Vorfall oder Incident auf die Geschäftsprozesse und die Gesamtorganisation haben kann. Im Kontext des Business Continuity Managements (BCM) ist das Verständnis des Business Impacts entscheidend, um angemessene Maßnahmen zur Aufrechterhaltung oder Wiederherstellung von Geschäftsprozessen zu planen.

Schritt 1: Identifikation der Geschäftsprozesse

- Prozessliste erstellen
  - Name des Prozesses
  - Zweck/Funktion
  - Beteiligte Abteilungen/MitarbeiterInnen
  - Input/Output des Prozesses.

Schritt 2: Ermittlung von potenziellen Incidents und Auswirkungen

- Potenzielle Incidents
  - Cyber-Security-Vorfälle (Hacking, Ransomware, Denial-of Service ...)
  - Naturkatastrophen und Umweltereignisse (Hochwasser, Blitzschlag...)
  - Technische Störungen und Ausfälle (Stromausfall, Netzwerkausfall...)
  - Menschliche Fehler (Fehlkonfiguration, Bedienfehler...)
  - Soziale und politische Vorfälle (Streiks, Anschläge...)
  - Sicherheitsvorfälle (Vandalismus, Diebstahl...)
  - Verlust von Schlüsselpersonal (Kündigung, plötzlicher Todesfall...)
  - Infrastrukturprobleme (Zugangsbeschränkungen, Gebäudeschäden...)
- Bewertung der Auswirkungen
  - Finanzielle Auswirkungen (Umsatzverlust, Vertragsstrafen...)
  - Operative Auswirkungen (Produktionsausfälle, Lieferverzögerung...)
  - Rechtliche Auswirkungen (Vertragsverletzungen, Geldstrafen...)
  - Reputationsschäden (Verlust des Kundenvertrauens...)

Schritt3: Quantifizieren des Impacts

- **Zeitlicher Rahmen**: Bestimmen Sie, wie sich die Auswirkungen über die Zeit entwickeln (z. B. nach 1 Stunde, 24 Stunden, 1 Woche).
- **Messgrößen festlegen**: Nutzen Sie Kennzahlen wie Umsatz pro Stunde/Tag, Anzahl betroffener Kunden oder Kosten pro Ausfallstunde.
- **Berechnung der finanziellen Verluste**: Multiplizieren Sie die Ausfallzeit mit den Kosten pro Zeiteinheit.

Schritt 4: Bestimmung der Kritikalität der Incidents

- **Recovery Time Objective (RTO):** Die maximale tolerierbare Ausfallzeit, bevor der Prozess wiederhergestellt sein muss.
- **Recovery Point Objective (RPO):** Der maximale tolerierbare Datenverlust in Bezug auf die Zeit.

Schritt 5: Erstellung eines Impact Scores:

Verwenden Sie eine Scoring-Methode, um Prozesse nach ihrem Impact zu bewerten (z. B. Skala von 1 bis 5). Berücksichtigen Sie verschiedene Kategorien (finanziell, operativ, reputativ) und gewichten Sie diese entsprechend ihrer Bedeutung.

Beispiel für einen Impact Score:

Kategorie	Gewichtung (%)	Bewertung (1-5)	Gewichteter Score
Finanziell	50%	4	2.0
Operativ	30%	3	0.9
Reputationsschaden	20%	2	0,4
Gesamtscore	**100%**		**3.3**

Interpretation: Ein Gesamtscore von 3.3 auf einer Skala von 1 bis 5 weist auf einen hohen Business Impact hin.

Schritt 6: Risikobewertung

- **Wahrscheinlichkeit des Auftretens**: Schätzen Sie ein, wie wahrscheinlich es ist, dass ein bestimmter Incident tatsächlich eintritt.
- **Risikoformel:**

Risiko = Wahrscheinlichkeit x Impact.

- **Priorisierung: Prozesse mit hohem Risiko und hohem Impact erhalten Priorität in der Planung.**

Fallbeispiel - Berechnung Business Impact

Ein mittelständisches Unternehmen wird Opfer eines Ransomware-Angriffs. Alle Server sind verschlüsselt, aber aktuelle Backups sind vorhanden. Die Wiederherstellung aller Systeme wird voraussichtlich 2 Tage dauern.

Berechnung des Business Impacts dieses Vorfalls, um die finanziellen und operativen Auswirkungen auf das Unternehmen zu quantifizieren.

In einer ersten Krisensitzung wird ermittelt, welche Auswirkungen dieser Incident auf ihre Geschäftstätigkeit haben wird:

Finanzielle Stabilität

- kurzfristige Liquiditätsengpässe durch verzögerte Zahlungseingänge
- langfristige Umsatzeinbußen durch Kundenverlust.

Operative Effizienz

- Produktionsausfälle führen zu Lieferengpässen.
- Störungen in der Lieferkette beeinträchtigen weitere Geschäftsbereiche.

Kundenbeziehungen

- Vertrauensverlust bei Kunden aufgrund von Serviceausfällen.
- Negative Mundpropaganda und mögliche Abwanderung.

Mitarbeitermoral

- Erhöhter Stress durch Krisenmanagement.
- Überstunden können zu Unzufriedenheit führen.

Compliance und Rechtliches

- Erhöhte Aufmerksamkeit von Regulierungsbehörden.
- Zukünftige Investitionen in Compliance-Maßnahmen erforderlich.

Schritt 1: Identifikation der betroffenen Geschäftsprozesse

- Vertrieb und Auftragserfassung
- Produktion
- Lagerverwaltung
- Versand und Logistik
- Kundenservice

- Finanz- und Rechnungswesen

Schritt 2: Ermittlung der Auswirkungen pro Geschäftsprozess

Auswirkungen auf die betroffenen Geschäftsprozesse:

- Vertrieb und Auftragserfassung
  - Keine neuen Aufträge können erfasst oder bearbeitet werden.
  - Durchschnittlicher Tagesumsatz: 100.000 €
- Produktion
  - Produktionsprozesse stehen still, da Maschinen IT-gestützt sind.
  - Tägliche Fixkosten der Produktion (Löhne, Abschreibungen): 50.000 €
- Lagerverwaltung
  - Kein Zugriff auf Lagerbestände; manuelle Prozesse sind ineffizient.
  - Zusätzliche Kosten durch manuellen Buchungen: 5.000 € pro Tag
- Versand und Logistik
  - Auslieferungen verzögern sich; Liefertermine können nicht eingehalten werden.
  - Mehrkosten durch Eil- und Sondertransporte: 10.000 € pro Tag
- Kundenservice
  - Kundenanfragen können nicht bearbeitet werden.
  - Potentieller Reputationsverlust: Schwer zu quantifizieren, aber zukünftige Umsatzverluste möglich.
- Finanz- und Rechnungswesen
  - Rechnungen können nicht gestellt oder Zahlungen verarbeitet werden.
  - Cashflow-Verzögerungen: 80.000 € pro Tag (Zahlungseingänge verschieben sich)

Schritt 3: Quantifizierung des Impacts

Direkte Verluste pro Tag:

1. Umsatzverlust im Vertrieb:	100.000 €
2. Produktionsfixkosten:	50.000 €
3. Zusätzliche Lagerkosten:	5.000 €
4. Eil- und Sondertransporte:	10.000 €
Summe der direkten Verluste pro Tag:	**165.000 €**

Direkte Verluste für 2 Tage:

165.000 € pro Tag x 2 Tage = **330.000 €**

Schritt 4: Quantifizierung der indirekten finanziellen Verluste

Reputationsschaden und zukünftiger Umsatzverlust

- Annahme: 5% der Kunden wechseln zur Konkurrenz aufgrund von Unzufriedenheit.
- Jährlicher Gesamtumsatz: 36.500.000 € (100.000 € x 365 Tage)
- Verlust durch Kundenabwanderung: 36.500.000 € x 5% = 1.825.000 €

Kosten für IT-Wiederherstellung und Sicherheitsverbesserungen

- IT-Personalüberstunden und externe Experten: 40.000 €
- Investitionen in neue Sicherheitslösungen: 60.000 €
- Gesamte IT-Kosten: 100.000 €

Rechtliche und regulatorische Kosten

- Mögliche Strafzahlungen aufgrund von Vertragsverletzungen: 50.000 €
- Anwalts- und Beratungskosten: 20.000 €
- Gesamte rechtliche Kosten: 70.000 €

Schritt 5: Gesamtkostenberechnung

1. Direkte finanzielle Verluste:	**330.000 €**
2. Indirekte finanzielle Verluste:	
- Reputationsschaden/Umsatzverlust:	1.825.000 €
- IT-Wiederherstellungs- und Verbesserungskosten:	100.000 €
- Rechtliche Kosten:	70.000 €
Summe der indirekten Verluste:	**1.995.000 €**
3. Gesamter Business Impact:	
330.000 € (direkte Verluste) + 1.995.000 € (indirekte Verluste) =	**2.325.000 €**

Schritt 6: Festlegung von Recovery Objectives

Recovery Time Objective (RTO)

- Ziel: Maximal zulässige Ausfallzeit von kritischen Systemen auf **12 Stunden** reduzieren.

Recovery Point Objective (RPO)

- Ziel: Maximal tolerierbarer Datenverlust **von 1 Stunde**.

Schritt 6: Risikobewertung

- **Wahrscheinlichkeit des Auftretens**: Schätzen Sie ein, wie wahrscheinlich es ist, dass ein bestimmter Incident tatsächlich eintritt. (z.B: 39% der KMUs erlitten 2019 durch Cyberangriffe einen tatsächlichen Schaden.

- **Risikoformel:**

Risiko = Wahrscheinlichkeit x Impact.

- **Priorisierung: Prozesse mit hohem Risiko und hohem Impact erhalten Priorität in der Planung.**

Schritt 7: Maßnahmen und Fazit

Der Ransomware-Angriff hat erhebliche finanzielle und operative Auswirkungen auf das Unternehmen mit einem geschätzten **Gesamtschaden von 2.325.000 €**. Durch gezielte Maßnahmen im Rahmen des Business Continuity Managements können zukünftige Risiken reduziert und die Resilienz des Unternehmens gesteigert werden.

- Verbesserung der IT-Sicherheitsmaßnahmen
  - Implementierung von Next-Generation-Firewalls und Anti-Ransomware-Software.
  - Regelmäßige Sicherheitsupdates und Patch-Management.
- Optimierung der Backup-Strategie
  - Echtzeit-Backups oder häufigere Backup-Intervalle.
  - Offsite- und Cloud-Backups zur zusätzlichen Sicherheit.
  - Regelmäßige Tests der Wiederherstellungsprozesse.
- Mitarbeiterschulung
  - Sensibilisierung für Cybersecurity-Risiken.
  - Schulungen zum Erkennen von Phishing-E-Mails und verdächtigen Aktivitäten.

- Notfallpläne und Business Continuity Planning
  - Erstellung von Notfallplänen für alle kritischen Geschäftsprozesse.
  - Definition von Ersatzprozessen, z. B. manuelle Auftragserfassung.
- Kommunikation
  - Transparente Information der Kunden über den Vorfall / getroffene Maßnahmen.
  - Interne Kommunikationsstrategie zur Koordination der Teams.
- Zusammenarbeit mit Behörden
  - Meldung des Vorfalls an zuständige Datenschutzbehörden.
  - Konsultation von Rechtsexperten für Compliance-Fragen.

Durch diese detaillierte Schritt-für-Schritt-Berechnung des Business Impacts erhält das Unternehmen eine klare Vorstellung von den finanziellen Konsequenzen eines Ransomware-Angriffs. Dies unterstreicht die Bedeutung proaktiver Maßnahmen im Bereich IT-Sicherheit und Business Continuity Management, um solche Risiken zu minimieren und die Geschäftsprozesse nachhaltig zu schützen.

BCM für Geschäftsprozesse

Beispielhafte BCM-Maßnahmen für spezifische Geschäftsprozesse:

- **Angebotserstellung:** Durch sichere Speicherung von Angebotsvorlagen und Kundendaten, z. B. in der Cloud oder auf redundanten Systemen, stellen Sie sicher, dass diese im Notfall zugänglich sind und der Verkaufsprozess nicht unterbrochen wird.
- **Auftragserfassung:** Die Einrichtung einer manuellen Auftragserfassung ermöglicht es, Bestellungen auch bei IT-Ausfällen zu bearbeiten, wodurch Umsatzverluste vermieden werden.
- **Kreditprüfung:** Alternative Verfahren, wie z. B. manuelle Bonitätsprüfungen oder Vorlagen für Standardkreditlimits, können den Verkaufsprozess aufrechterhalten, wenn das IT-System nicht verfügbar ist.
- **Lagerverwaltung:** Manuelle Lagerlisten oder Backup-Systeme helfen, den Überblick über Lagerbestände zu behalten und Lieferengpässe zu vermeiden.
- **Beschaffung:** Das Identifizieren alternativer Lieferanten und das Vorhalten eines Sicherheitsbestands an kritischen Materialien sichern die Produktion und Lieferfähigkeit.
- **Auftragsplanung/-steuerung:** Ein manueller Planungsprozess stellt sicher, dass Produktionsabläufe auch ohne IT-Unterstützung koordiniert werden können.
- **Qualitätskontrolle:** Durch alternative Qualitätsprüfungen, die nicht auf IT-Systeme angewiesen sind, bleibt die Produktqualität gewährleistet.

- **Kommissionierung und Verpackung & Versand:** Manuelle Prozesse in der Kommissionierung und ausreichende Vorräte an Verpackungsmaterialien ermöglichen weiterhin termingerechte Lieferungen.
- **Export- & Zollabwicklung:** Die Sicherung wichtiger Dokumente und Unterlagen stellt sicher, dass internationale Lieferungen nicht ins Stocken geraten.
- **Fakturierung und Zahlungseingang:** Manuelle Fakturierung und alternative Zahlungsmethoden sichern den Cashflow und die finanzielle Stabilität des Unternehmens.

Durch die Umsetzung von präventiven und reaktiven Maßnahmen können KMU ihre Geschäftsprozesse widerstandsfähiger gegen Störungen machen. BCM ermöglicht es, schnell auf unvorhergesehene Ereignisse zu reagieren, die Auswirkungen auf den Geschäftsbetrieb zu minimieren und die Kontinuität des Unternehmens zu gewährleisten. Dies ist nicht nur für die kurzfristige Problembewältigung wichtig, sondern trägt auch langfristig zur Stabilität der Geschäftsprozesse des Unternehmens bei.

Relevante Standards, Normen und Richtlinien

Internationale Standards

ISO 22301 Business continuity management systems

Die ISO 22301 ist die wichtigste internationale Norm für BCM. Sie definiert Anforderungen an ein Business Continuity Management System (BCMS) und bietet einen Rahmen für die Planung, Implementierung, Überwachung, Überprüfung und Verbesserung von BCM-Prozessen.

ISO 22313 - Guidance on the use of ISO 22301

Diese Norm bietet Leitlinien zur Anwendung der ISO 22301 und enthält zusätzliche Informationen und Empfehlungen für die Implementierung eines BCMS.

ISO 27001 - Informationssicherheit, Cybersicherheit und Datenschutz

Die ISO 27001 befasst sich mit dem Informationssicherheitsmanagement. Sie ist zwar nicht direkt auf BCM fokussiert, aber viele der darin enthaltenen Anforderungen sind auch für BCM relevant, insbesondere im Bereich der IT-Sicherheit und des Datenschutzes.

Nationale Standards & Richtlinien

BSI-Standard 200-4: Business Continuity Management (BCM)

Der deutsche BSI-Standard 200-4 bietet eine praxisnahe Anleitung zum Aufbau und zur Etablierung eines BCMS. Er basiert auf der ISO 22301 und ist speziell auf die Bedürfnisse deutscher Unternehmen zugeschnitten.

Österreichisches Informationssicherheitshandbuch

Das Österreichische Informationssicherheitshandbuch ist ein umfassender Leitfaden, der von der österreichischen Bundesregierung herausgegeben wird. Es bietet Unternehmen und Organisationen detaillierte Anleitungen und Empfehlungen zur Implementierung und Verbesserung ihrer Informationssicherheit.

https://www.sicherheitshandbuch.gv.at/

Gesetze & Verordnungen

Netz- und Informationssystemsicherheitsgesetz

Das IT-Sicherheitsgesetz verpflichtet Betreiber kritischer Infrastrukturen zum Ergreifen von Sicherheitsmaßnahmen und zur Erstellung von Notfallplänen. Dies ist auch für Logistikunternehmen relevant, die zur kritischen Infrastruktur gehören (z.B. Transport von lebenswichtigen Gütern).

Datenschutzgrundverordnung (DSGVO)

Die DSGVO enthält Anforderungen an den Schutz personenbezogener Daten. Im Rahmen von BCM müssen Unternehmen sicherstellen, dass auch im Krisenfall der Datenschutz gewährleistet ist.

Weitere relevante Aspekte

Versicherungspflichten

In einigen Branchen bestehen gesetzliche Versicherungspflichten, die auch die Absicherung von Betriebsunterbrechungen umfassen können.

Vertragliche Verpflichtungen

Unternehmen können auch vertragliche Verpflichtungen zum BCM haben, z.B. gegenüber Kunden oder Geschäftspartnern.

Beachten Sie: Die genannten Richtlinien, Verordnungen, Standards und Gesetze stellen nur einen Auszug dar. Die konkreten Anforderungen können je nach Branche, Unternehmensgröße und Tätigkeit variieren. Es ist wichtig, sich regelmäßig über neue und geänderte Vorschriften zu informieren.

Checkliste zur Umsetzung von BCM in KMU

Da Sie Ihre kritischen Geschäftsprozesse definiert haben, konzentrieren wir uns nun auf konkrete Maßnahmen, die KMU im BCM ergreifen können, um auf Cyberangriffe, Stromausfälle und IT-Probleme vorbereitet zu sein.

Präventive Maßnahmen

Risikoanalyse: Identifizieren und bewerten Sie potenzielle Cyberrisiken, Schwachstellen in der IT-Infrastruktur und die Auswirkungen von Stromausfällen auf Ihre Geschäftsprozesse.	☐
Datensicherung: Richten Sie ein robustes System zur Datensicherung ein, das regelmäßige Backups, redundante Speichermedien und Offsite-Backups umfasst.	☐
Cyber-Security: Implementieren Sie Firewalls, Virenschutzsoftware, Intrusion Detection Systeme und andere Sicherheitsmaßnahmen zum Schutz vor Cyberangriffen.	☐
Zugangskontrolle: Verwenden Sie starke Passwörter, Multi-Faktor-Authentifizierung und Zugriffsberechtigungen, um den unbefugten Zugriff auf IT-Systeme und Daten zu verhindern.	☐
Software-Updates: Installieren Sie regelmäßig Software-Updates und Sicherheits-Patches, um bekannte Schwachstellen zu schließen.	☐
Schulung der Mitarbeiter: Sensibilisieren Sie Ihre Mitarbeiter für Cyber-Security-Risiken und schulen Sie sie im Umgang mit verdächtigen E-Mails, Phishing-Versuchen und anderen Bedrohungen.	☐
Notstromversorgung: Sichern Sie die Stromversorgung kritischer IT-Systeme und Anlagen durch Notstromaggregate oder USV-Anlagen.	☐
Redundante Systeme: Setzen Sie redundante Server, Netzwerkkomponenten und andere IT-Systeme ein, um Ausfälle einzelner Komponenten zu kompensieren.	☐
Cloud-Lösungen: Nutzen Sie Cloud-Lösungen für die Datenspeicherung, Anwendungsbereitstellung und andere IT-Services, um die Verfügbarkeit und Skalierbarkeit zu erhöhen.	☐
Mobile Arbeitsplätze:Richten Sie mobile Arbeitsplätze ein, damit Mitarbeiter im Falle eines Stromausfalls oder IT-Problems von zu Hause oder einem anderen Ort aus arbeiten können.	☐
Dokumentation: Dokumentieren Sie Ihre IT-Systeme, Netzwerkarchitektur und Notfallprozesse, um im Krisenfall schnell reagieren zu können.	☐

Reaktive Maßnahmen

Notfallplan: Erstellen Sie einen detaillierten Notfallplan, der die Schritte zur Reaktion auf Cyberangriffe, Stromausfälle und IT-Probleme beschreibt.	☐
Kommunikationsplan: Definieren Sie Kommunikationswege und -verantwortlichkeiten im Krisenfall, um die interne und externe Kommunikation sicherzustellen.	☐
Incident Response Team: Bilden Sie ein Incident Response Team, das im Falle eines Cyberangriffs oder IT-Problems die notwendigen Maßnahmen ergreift.	☐
Datenwiederherstellung: Testen Sie regelmäßig die Wiederherstellung von Daten aus Backups, um sicherzustellen, dass die Daten im Notfall schnell und vollständig wiederhergestellt werden können.	☐
Alternative Kommunikationswege: Richten Sie alternative Kommunikationswege ein (z. B. Telefon, Fax, Messenger), falls die primären Kommunikationskanäle ausfallen.	☐
Manuelle Prozesse: Definieren Sie manuelle Prozesse oder Workarounds für kritische Geschäftsprozesse, die im Falle eines IT-Ausfalls durchgeführt werden können.	☐
Externe Dienstleister: Identifizieren Sie externe Dienstleister, die im Krisenfall Unterstützung leisten können (z. B. IT-Support, Datenrettung).	☐

Spezifische Maßnahmen für Ihre Geschäftsprozesse

Angebotserstellung: Speichern Sie Angebotsvorlagen und Kundendaten sicher und stellen Sie sicher, dass diese im Notfall zugänglich sind.	☐
Auftragserfassung: Ermöglichen Sie die manuelle Auftragserfassung, falls das IT-System ausfällt.	☐
Kreditprüfung: Definieren Sie alternative Verfahren zur Kreditprüfung, falls der Zugriff auf das IT-System nicht möglich ist.	☐
Lagerverwaltung: Führen Sie manuelle Lagerlisten oder verwenden Sie ein Backup-System, um die Lagerbestände im Notfall zu verwalten.	☐
Beschaffung: Identifizieren Sie alternative Lieferanten und halten Sie einen Sicherheitsbestand an kritischen Materialien.	☐
Auftragsplanung/-steuerung: Erstellen Sie einen manuellen Planungsprozess, falls das IT-System nicht verfügbar ist.	☐
Qualitätskontrolle: Definieren Sie alternative Verfahren zur Qualitätskontrolle, die auch ohne IT-Unterstützung durchgeführt werden können.	☐
Kommissionierung: Ermöglichen Sie die manuelle Kommissionierung von Aufträgen.	☐
Verpackung & Versand: Halten Sie ausreichend Verpackungsmaterial und Versanddokumente bereit.	☐
Export- & Zollabwicklung: Sichern Sie Exportdokumente und Zollunterlagen und stellen Sie sicher, dass diese im Notfall zugänglich sind.	☐
Fakturierung: Ermöglichen Sie die manuelle Fakturierung von Aufträgen.	☐
Zahlungseingang: Richten Sie alternative Zahlungsmethoden ein (z. B. Barzahlung, Überweisung).	☐

Zusätzliche Tipps

Testen und Üben: Führen Sie regelmäßig Notfallübungen durch, um die Wirksamkeit Ihrer BCM-Maßnahmen zu überprüfen und die Reaktionsfähigkeit Ihrer Mitarbeiter zu trainieren.	☐
Kontinuierliche Verbesserung: Überprüfen und aktualisieren Sie Ihre BCM-Pläne und -Prozesse regelmäßig, um sie an veränderte Bedingungen anzupassen.	☐
Dokumentation: Halten Sie Ihre BCM-Dokumentation aktuell und stellen Sie sicher, dass sie im Notfall leicht zugänglich ist.	☐

Auswertung

Gehen Sie die Checkliste durch und vergeben Sie für jedes erfüllte Kriterium einen Punkt. Summieren Sie anschließend die Punkte und ermitteln Sie Ihre Punktzahl.

- **27–33 Punkte**: **Sehr hohe BC** – Ihr Unternehmen ist hervorragend auf Krisen vorbereitet.
- **26–21 Punkte**: **Hohe BC** – Sie sind gut aufgestellt, es gibt jedoch Optimierungspotenzial.
- **20–15 Punkte**: **Mittlere BC** – Identifizieren Sie Bereiche mit Handlungsbedarf.
- **0–15 Punkte**: **Geringe BC** – Es besteht dringender Verbesserungsbedarf.

Wichtige Hinweise

- Diese Skala dient als Orientierungshilfe und ersetzt kein umfassendes BCM
- Die Gewichtung der einzelnen Kriterien kann je nach Branche und Unternehmen variieren.
- Es ist wichtig, die Ergebnisse der Bewertung zu analysieren und konkrete Maßnahmen zur Verbesserung des BCM abzuleiten.

Nächste Schritte

- Identifizieren Sie Schwachstellen: Schauen Sie sich die nicht angekreuzten Punkte an und priorisieren Sie diese nach deren Einfluss auf Ihr Geschäft.
- Erstellen Sie einen Aktionsplan: Definieren Sie konkrete Maßnahmen, Verantwortliche und Zeitpläne für die Umsetzung.
- Kontinuierliche Überprüfung: Integrieren Sie diese Checkliste in Ihre regelmäßigen Managementprozesse, um die Robustheit Ihrer Lieferkette dauerhaft zu sichern.
- Diese Checkliste dient als Ausgangspunkt für eine umfassende Bewertung und sollte an die spezifischen Gegebenheiten Ihres Unternehmens angepasst werden.

Fazit & Ausblick

Business Continuity Management (BCM) ermöglicht es Unternehmen, auch in Krisenzeiten handlungsfähig zu bleiben. Durch die Implementierung von BCM-Maßnahmen können Unternehmen ihre Widerstandsfähigkeit gegenüber Störungen erhöhen und sicherstellen, dass kritische Geschäftsprozesse auch im Notfall weiterlaufen.

Zukünftig wird BCM aufgrund zunehmender Cyber-Risiken und globaler Unsicherheiten noch wichtiger werden. Unternehmen müssen daher verstärkt in präventive Maßnahmen investieren und ihre BCM-Strategien kontinuierlich anpassen. Dazu gehört die Sensibilisierung der Mitarbeiter für Cyber-Security, die Implementierung von Notfallplänen und die regelmäßige Überprüfung der BCM-Prozesse.

Die Investition in BCM ist eine Investition in die Zukunftssicherheit von Unternehmen. Nur wer auf Krisen vorbereitet ist, kann langfristig erfolgreich sein.

Weitere Informationen finden Sie in unseren Leitfäden:

ReLief4U - Leitfaden No 1: Risikoanalyse und -bewertung in der Lieferkette

Der "ReLief4U - Leitfaden No 1: Risikoanalyse und -bewertung in der Lieferkette" bietet KMUs eine praxisnahe Anleitung zur Stärkung ihrer Resilienz. Erfahren Sie, wie Sie potenzielle Risiken in Kategorien wie Beschaffung, Produktion und Logistik identifizieren und bewerten. Anhand konkreter Beispiele aus dem VNL-Projekt SRCM lernen Sie, die Auswirkungen von Störungen auf Ihre Geschäftsprozesse zu analysieren. Mittels Checklisten und bewährten Methoden können Sie Risiken priorisieren und gezielt Maßnahmen zur Risikominimierung ergreifen. So sichern Sie die Stabilität Ihrer Lieferkette und steigern Ihre Wettbewerbsfähigkeit.

ReLief4U - Leitfaden No 2: Robuste Lieferketten: Der Schlüssel zur Resilienz

Der zweite Teil konzentriert sich auf die Erhöhung der Robustheit der Lieferketten. Hier werden Maßnahmen vorgestellt, die darauf abzielen, die Lieferkette gegen häufige und vorhersehbare Störungen abzusichern. Dazu gehören die Diversifizierung der Lieferantenbasis, die Einführung von Sicherheitsbeständen und die Implementierung redundanter Systeme. Praktische Anleitungen und konkrete Beispiele zeigen, wie KMUs diese Strategien effektiv umsetzen können, um eine stabile und widerstandsfähige Lieferkette zu schaffen. Der Fokus liegt darauf, Schwachstellen zu identifizieren und durch gezielte Maßnahmen die Widerstandsfähigkeit der Lieferkette zu stärken.

ReLief4U - Leitfaden No 3: Agile Lieferketten gestalten: Ein Praxisleitfaden für KMUs

Auf der Grundlage der robusten Strukturen widmet sich der zweite Teil der Steigerung der Agilität der Lieferkette. Agilität ermöglicht es Unternehmen, schnell und flexibel auf unvorhergesehene Veränderungen und Marktanforderungen zu reagieren. Dieser Abschnitt

behandelt Methoden wie die Einführung flexibler Produktionsprozesse, den Einsatz von Echtzeit-Datenanalyse und die Förderung einer innovationsfreundlichen Unternehmenskultur. Durch konkrete Fallbeispiele und Schritt-für-Schritt-Anleitungen lernen KMUs, wie sie ihre Lieferketten agil gestalten können, um sich dynamischen Marktbedingungen anzupassen und Wettbewerbsvorteile zu sichern.

ReLief4U - Leitfaden No. 4: Business Continuity Management: Ein Leitfaden für KMUs

Der vierte Teil fokussiert sich auf die Einführung eines Business Continuity Managements (BCM). BCM umfasst die systematische Planung und Vorbereitung auf schwerwiegende Störungen und Krisensituationen. Dieser Abschnitt beschreibt die Entwicklung von Notfallplänen, die Durchführung regelmäßiger Risikoanalysen und die Etablierung von Krisenmanagement-Teams. KMUs erfahren, wie sie BCM-Prozesse integrieren können, um sicherzustellen, dass kritische Geschäftsprozesse auch unter extremen Bedingungen aufrechterhalten werden. Praktische Anleitungen und Checklisten unterstützen die Implementierung dieser Maßnahmen im Unternehmensalltag.

Weiterführende Literatur

1. Arndt, Holger (2021): Supply Chain Management. Wiesbaden: Springer Fachmedien Wiesbaden.
2. Beisswenger, Philipp; Recknagel, Robert (2023): Wirksame Strategien gegen schwarze Schwäne. In: Peter H. Voß (Hg.): Die Neuerfindung der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 19–26.
3. Biedermann, Lukas (2018): Supply Chain Resilienz. Konzeptioneller Bezugsrahmen und Identifikation Zukünftiger Erfolgsfaktoren. Wiesbaden: Gabler. Online verfügbar unter https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5507918.
4. Blyth, Michael (2009): Business continuity management. Building an effective incident management plan. Hoboken, NJ: Wiley. Online verfügbar unter http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10308147.
5. Brühwiler, Bruno (2016): Notwendigkeit und Nutzen von internationalen Standards im Logistik-Risikomanagement. In: Michael Huth und Frank Romeike (Hg.): Risikomanagement in der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 159–169.
6. Dovbischuk, Irina; Siestrup, Guido; Tuma, Axel (Hg.) (2018): Nachhaltige Impulse für Produktion und Logistikmanagement. Wiesbaden: Springer Fachmedien Wiesbaden.
7. Engelhardt-Nowitzki, Corinna (Hg.) (2010): Supply Chain Network Management. Gestaltungskonzepte und Stand der praktischen Anwendung. 1. Aufl. Wiesbaden: Gabler (Gabler Research).
8. Friesz, Alexander (2023): Die Logistik auf dem Weg ins 22. Jahrhundert. In: Peter H. Voß (Hg.): Die Neuerfindung der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 179–194.
9. Fürbacher, Jörg; Lagally, Thomas (2023): Die vernetzte und intelligente Transportmanagement-Plattform – Basis der digitalen Resilienz. In: Andrea Lochmahr und Marcus Ewig (Hg.): Praxishandbuch digitale Automobillogistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 185–197.
10. Habermann, Mandy; Schauberger, Katharina; Sternbeck, Michael (2024): Die Verwundbarkeit globaler Lieferketten und betriebliche Ansatzpunkte in Supply Chain Management und Finance zur Steigerung der Resilienz. In: Marc Knoppe (Hg.): Unternehmerische Wertschöpfung neu aufstellen. Wiesbaden: Springer Fachmedien Wiesbaden, S. 85–119.
11. Hänggi, Roman; Luban, Katharina; Bernard, Giuliano (2022): Stärkung der Resilienz in Unternehmen: Das Rapperswiler Resilienzmodell. In: Katharina Luban und Roman Hänggi (Hg.): Erfolgreiche Unternehmensführung durch Resilienzmanagement. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 245–264.
12. Helmold, Marc (2023): Wettbewerbsvorteile entlang der Supply Chain sichern. Best-Practice-Beispiele in Beschaffung, Produktion, Marketing und anderen Funktionen der betriebswirtschaftlichen Wertschöpfungskette. Wiesbaden, Heidelberg: Springer Gabler. Online verfügbar unter http://www.springer.com/.

13. Helmold, Marc (2024): Digitalisierung und KI-Anwendungen im Supply Chain Management (SCM). In: Marc Helmold (Hg.): Erfolgreiche Transformation zum digitalen Champion. Wiesbaden: Springer Fachmedien Wiesbaden, S. 167–177.

14. Helmold, Marc (Hg.) (2024): Erfolgreiche Transformation zum digitalen Champion. Wiesbaden: Springer Fachmedien Wiesbaden.

15. Heß, Gerhard; Kleinlein, Ann-Christin (Hg.) (2021): Resilienz im Einkauf. Wiesbaden: Springer Fachmedien Wiesbaden.

16. Heß, Gerhard; Kleinlein, Ann-Christin (2021): Resilienz im Einkauf durch Krisenmanagement. In: Gerhard Heß und Ann-Christin Kleinlein (Hg.): Resilienz im Einkauf. Wiesbaden: Springer Fachmedien Wiesbaden, S. 61–110.

17. Hirth, Stefan; Markert, Timo (2023): Mit Resilienz-Strategien Krisen meistern – „Effective crisis management is king, communication is queen." (Stefan Hirth). In: Stefan Hirth und Timo Markert (Hg.): Neue Perspektiven auf Strategie und Innovation. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 107–124.

18. Hirth, Stefan; Markert, Timo (Hg.) (2023): Neue Perspektiven auf Strategie und Innovation. Berlin, Heidelberg: Springer Berlin Heidelberg.

19. Hoff, Stefan; Kahrs, Carsten; Keller, Fabian (2023): Die Organisation für die digitalisierte Supply Chain von Morgen. In: Andrea Lochmahr und Marcus Ewig (Hg.): Praxishandbuch digitale Automobillogistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 41–54.

20. Hohmann, Susanne (Hg.) (2022): Logistik- und Supply Chain Management. Wiesbaden: Springer Fachmedien Wiesbaden.

21. Hohmann, Susanne (2022): Supply Chain Management. In: Susanne Hohmann (Hg.): Logistik- und Supply Chain Management. Wiesbaden: Springer Fachmedien Wiesbaden, S. 195–255.

22. Huth, Michael; Romeike, Frank (Hg.) (2016): Risikomanagement in der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden.

23. Ivanov, Dmitry (2023): Einführung in die Widerstandsfähigkeit der Lieferkette. Cham: Springer International Publishing.

24. Kamala Raman and Daniel Ryntjes (2020): The Route to a More Resilient Supply Chain. In: *Gartner Business Quarterly* (Q4).

25. Kleemann, Florian C.; Frühbeis, Ronja (2021): Grundlagen von Resilienz und Supply Chain Management. In: Florian C. Kleemann und Ronja Frühbeis (Hg.): Resiliente Lieferketten in der VUCA-Welt. Wiesbaden: Springer Fachmedien Wiesbaden (essentials), S. 3–8.

26. Kleemann, Florian C.; Frühbeis, Ronja (Hg.) (2021): Resiliente Lieferketten in der VUCA-Welt. Wiesbaden: Springer Fachmedien Wiesbaden (essentials).

27. Kleemann, Florian C.; Frühbeis, Ronja (2021): Resiliente Lieferketten in der VUCA-Welt. Wiesbaden: Springer Fachmedien Wiesbaden.

28. Kleemann, Florian C.; Frühbeis, Ronja (2021): Supply-Chain-Disruptionen in der VUCA-Welt. In: Florian C. Kleemann und Ronja Frühbeis (Hg.): Resiliente Lieferketten in der VUCA-Welt. Wiesbaden: Springer Fachmedien Wiesbaden (essentials), S. 9–18.

29. Klepzig, Heinz-Jürgen (Hg.) (2023): Financial Supply Chain. Wiesbaden: Springer Fachmedien Wiesbaden.

30. Klepzig, Heinz-Jürgen (2023): Risikomanagement und Resilienz. In: Heinz-Jürgen Klepzig (Hg.): Financial Supply Chain. Wiesbaden: Springer Fachmedien Wiesbaden, S. 249–289.

31. Knoppe, Marc (Hg.) (2024): Unternehmerische Wertschöpfung neu aufstellen. Wiesbaden: Springer Fachmedien Wiesbaden.

32. Kollatz, Peter; Wicke, Thomas (2020): Neue Sicherheitsherausforderungen für die Logistik. In: Peter H. Voß (Hg.): Logistik – die unterschätzte Zukunftsindustrie. Wiesbaden: Springer Fachmedien Wiesbaden, S. 179–188.

33. Krauss, Sabrina; Plugmann, Philipp (Hg.) (2022): Innovationen in der Wirtschaft. Wiesbaden: Springer Fachmedien Wiesbaden.

34. Kremer, Roman Bruno (2022): Resiliente Supply Chains und der Faktor Mensch: Digitalisierung und Automatisierung im Rahmen innovativer Logistikkonzepte in Krisenzeiten. In: Sabrina Krauss und Philipp Plugmann (Hg.): Innovationen in der Wirtschaft. Wiesbaden: Springer Fachmedien Wiesbaden, S. 77–90.

35. Lasch, Rainer (2023): Strategisches und operatives Logistikmanagement: Prozesse. 4., überarbeitete Auflage. Wiesbaden: Springer Gabler.

36. Linnemann, Matthias; Bahner, Andreas; Bremer, Georg (2023): Mögliche Wirklichkeiten – Wohl und Übel von Lieferketten. In: Matthias Linnemann, Andreas Bahner und Georg Bremer (Hg.): Umgang mit Krisenauswirkungen in der Bauwirtschaft. Wiesbaden: Springer Fachmedien Wiesbaden (essentials), S. 3–12.

37. Linnemann, Matthias; Bahner, Andreas; Bremer, Georg (Hg.) (2023): Umgang mit Krisenauswirkungen in der Bauwirtschaft. Wiesbaden: Springer Fachmedien Wiesbaden (essentials).

38. Lochmahr, Andrea; Ewig, Marcus (Hg.) (2023): Praxishandbuch digitale Automobillogistik. Wiesbaden: Springer Fachmedien Wiesbaden.

39. Luban, Katharina; Hänggi, Roman (Hg.) (2022): Erfolgreiche Unternehmensführung durch Resilienzmanagement. Berlin, Heidelberg: Springer Berlin Heidelberg.

40. Maximilian Festus (2024): "Frühzeitige Maßnahmen stärken Lieferketten-Resilienz". In: *Produktion* (13), S. 5. Online verfügbar unter https://www.wiso-net.de/document/PROD__A125595983.

41. Milkau, Udo (2022): Industrielle Implementierungen von Operational Resilience. In: Udo Milkau (Hg.): Operational Resilience in Finanzinstituten. Wiesbaden: Springer Fachmedien Wiesbaden, S. 107–130.

42. Milkau, Udo (Hg.) (2022): Operational Resilience in Finanzinstituten. Wiesbaden: Springer Fachmedien Wiesbaden.

43. Müller, Rainer; Meyer-Larsen, Nils; Lange, Felix (2018): Resiliente intermodale Transporte – Gesundheits-Check-up für Supply Chains. In: Irina Dovbischuk, Guido Siestrup und Axel Tuma (Hg.): Nachhaltige Impulse für Produktion und Logistikmanagement. Wiesbaden: Springer Fachmedien Wiesbaden, S. 87–95.

44. Pedell, Burkhard; Gleißner, Werner; Kühlem, Melanie Christine; Nickel, Johannes (2024): Resilienz- und Risikomanagement in der Wertschöpfungskette. In: *Control Manag Rev* 68 (1), S. 8–17. DOI: 10.1007/s12176-023-1100-6.

45. Röhe, Achim (Hg.) (2022): Das resiliente Unternehmen – Die Krisen der Zukunft erfolgreich meistern. Berlin, Heidelberg: Springer Berlin Heidelberg.

46. Röhe, Achim (2022): Das resiliente Unternehmen entsteht. In: Achim Röhe (Hg.): Das resiliente Unternehmen – Die Krisen der Zukunft erfolgreich meistern. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 115–165.

47. Romeike, Frank; Hager, Peter (Hg.) (2020): Erfolgsfaktor Risiko-Management 4.0. Wiesbaden: Springer Fachmedien Wiesbaden.

48. Romeike, Frank; Hager, Peter (2020): Risiko-Management in der Produktion. In: Frank Romeike und Peter Hager (Hg.): Erfolgsfaktor Risiko-Management 4.0. Wiesbaden: Springer Fachmedien Wiesbaden, S. 297–351.

49. Romeike, Frank; Spitzner, Jan (2016): Einsatz von Simulationsmethoden im Logistik-Risikomanagement. In: Michael Huth und Frank Romeike (Hg.): Risikomanagement in der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 127–158.

50. Roselieb, Frank (2022): Business Continuity Management in der Praxis. Mit Krisen professionell umgehen - erfolgreiche Konzepte und Fallbeispiele. Unter Mitarbeit von Franziskus Bayer, Florian Feldbauer, Werner Gleißner, Lars Halbauer, Ulrich Heuer, Melanie Kamann et al. 1st ed. Berlin: Erich Schmidt Verlag. Online verfügbar unter https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=7024627.

51. Rühl, Uwe (2021): Der Lebenszyklus des Business-Continuity-Managements. In: Uwe Rühl (Hg.): Quick Guide Erfolgreiches Business-Continuity-Management. Berlin, Heidelberg: Springer Berlin Heidelberg (Quick Guide), S. 27–44.

52. Rühl, Uwe (2021): Quick Guide Erfolgreiches Business-Continuity-Management. Wie Sie Geschäftsunterbrechungen überleben und Gestärkt in Die Zukunft Gehen. Berlin, Heidelberg: Springer Berlin / Heidelberg (Quick Guide Ser). Online verfügbar unter https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6727145.

53. Rühl, Uwe (Hg.) (2021): Quick Guide Erfolgreiches Business-Continuity-Management. Berlin, Heidelberg: Springer Berlin Heidelberg (Quick Guide).

54. Schuh, Günther; Stich, Volker (Hg.) (2013): Logistikmanagement. Berlin, Heidelberg: Springer Berlin Heidelberg.

55. Schwemmer, Martin (2021): Auf dem Weg zu einer Neuen Logistik. In: Martin Schwemmer und Patrick Seeßle (Hg.): Logistik-Start-ups. Wiesbaden: Springer Fachmedien Wiesbaden, S. 13–30.

56. Schwemmer, Martin; Seeßle, Patrick (Hg.) (2021): Logistik-Start-ups. Wiesbaden: Springer Fachmedien Wiesbaden.

57. Spörrer, Stefan (2014): Business Continuity Management. ISO 22301 und weitere Normen im Rahmen der Informationstechnologie. Wiesbaden: Springer Fachmedien Wiesbaden (SpringerLink Bücher).

58. Stich, Volker; Quick, Jerome; Cuber, Stefan (2013): Konfiguration logistischer Netzwerk. In: Günther Schuh und Volker Stich (Hg.): Logistikmanagement. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 35–75.

59. Stich, Volker; Reschke, Jan; Holtkemper, David; Kraut, Andreas; Pause, Daniel; Marek, Svenja (2020): Digitalisierung der Supply-Chain. In: Peter H. Voß (Hg.): Logistik – die unterschätzte Zukunftsindustrie. Wiesbaden: Springer Fachmedien Wiesbaden, S. 17–32.

60. Stich, Volker; Schröer, Tobias; Linnartz, Maria; Janßen, Jokim (2023): Resilienz jetzt – Wie Krisen unseren Blick auf Wertschöpfungsnetzwerke verändern. In: Peter H. Voß (Hg.): Die Neuerfindung der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 41–49.

61. Sucky, Eric (2021): Supply Chain Management. 1st ed. Stuttgart: Kohlhammer Verlag. Online verfügbar unter https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6803189.

62. Treier, Volker und Carolin Herweg (2022): Globale Lieferketten unter Druck. In: *Ifo schnelldienst* (Bd. 75, Nr. 1), S. 8–11.

63. Unkrig, Erich R. (2020): Agilität durch gelebte Prinzipien und Werte. In: Erich R. Unkrig (Hg.): Mandate der Führung 4.0. Wiesbaden: Springer Fachmedien Wiesbaden, S. 83–137.

64. Unkrig, Erich R. (Hg.) (2020): Mandate der Führung 4.0. Wiesbaden: Springer Fachmedien Wiesbaden.

65. Voß, Peter H. (Hg.) (2020): Logistik – die unterschätzte Zukunftsindustrie. Wiesbaden: Springer Fachmedien Wiesbaden.

66. Voß, Peter H. (Hg.) (2023): Die Neuerfindung der Logistik. Wiesbaden: Springer Fachmedien Wiesbaden.

67. Wellbrock, Wanja: Ganzheitliches Risikomanagement in der Lieferkette – Strategisches Potenzial des Lieferkettensorgfaltspflichtengesetzes. In: *Ifo schnelldienst* 2022 (Bd. 75, Nr. 1), S. 12–15.

68. Werner, Hartmut (2020): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 7., vollständig überarbeitete und erweiterte Auflage. Wiesbaden: Springer Gabler (Springer eBook Collection).

69. Werner, Hartmut (2022): Supply Chains resilienter aufstellen. In: *Control Manag Rev* 66 (5), S. 42–47. DOI: 10.1007/s12176-022-0480-3.

Verein Netzwerk Logistik

Wolfernstrasse 39, 4400 Steyr

+43 7252 98 281 6100

office@vnl.at

www.vnl.at