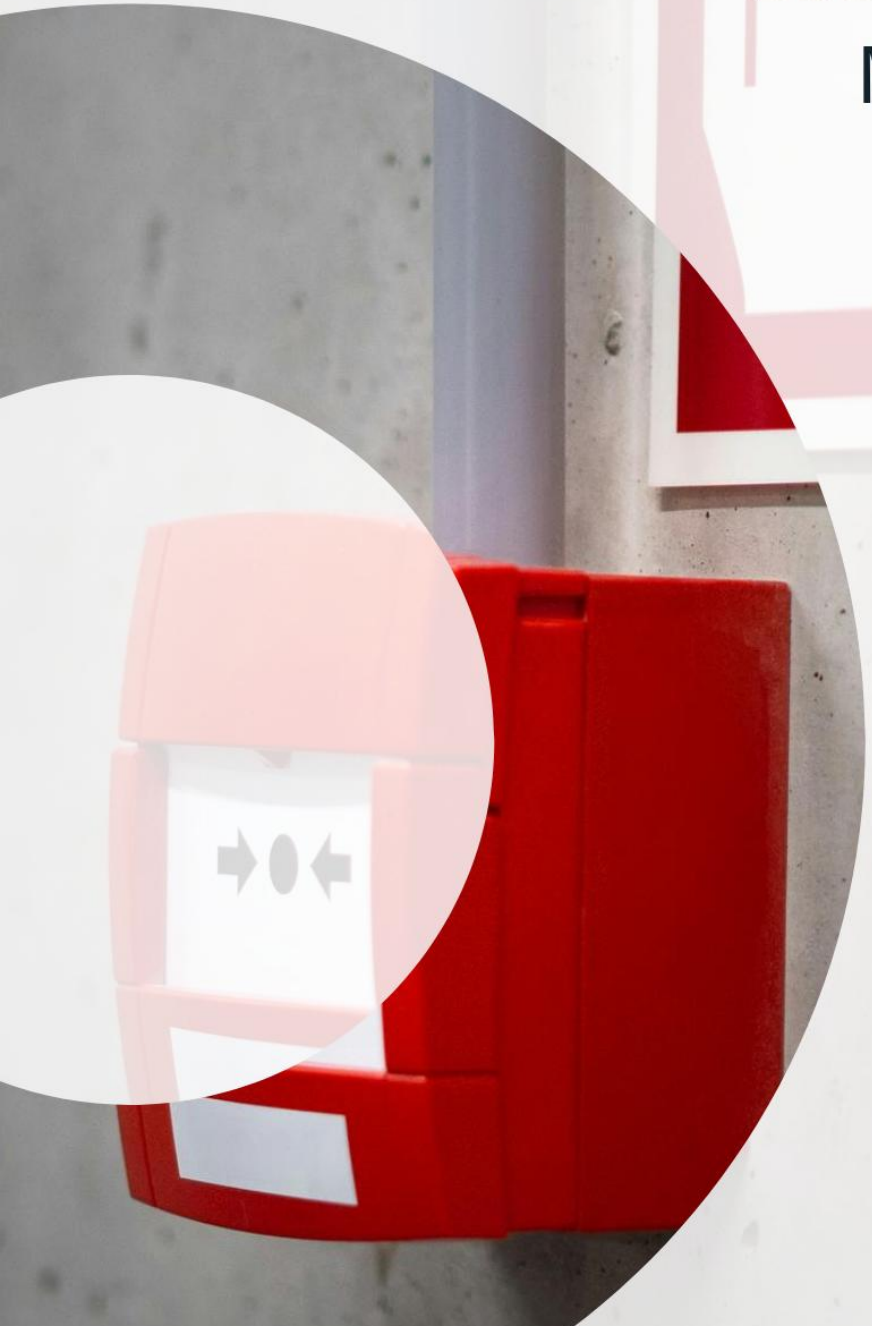
TEXSUS

LEITFADEN

BUSINESS CONTINUITY MANAGEMENT UND BRANDSCHUTZ



INTRASYS

gefördert durch DBU Deutsche Bundesstiftung Umwelt

HOCHSCHULE LANDSHUT

DTV DEUTSCHER TEXTILREINIGUNGS VERBAND

DISCLAIMER: *Aus Lesbarkeitsgründen wird in diesem Leitfaden auf die verschiedene Ansprechweisen, sei es divers, männlich oder weiblich verzichtet. Alle Formulierungen sprechen gleichermaßen alle Geschlechter an und sind im generischen Maskulinum formuliert*

AUTOREN

INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH
Dipl.-Betriebswirt (FH) Klaus Eder



Klaus Eder ist geschäftsführender Gesellschafter der INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH, Landshut. Seine Tätigkeitsschwerpunkte liegen neben dem Projektmanagement in der Einführung und Optimierung von Managementsystemen. Seit 1999 nimmt er Lehraufträge an der Hochschule Landshut wahr.

INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH
Dipl.-Betriebswirt Oliver Lehmann



Oliver Lehmann ist seit über 20 Jahren als Unternehmensberater bei der INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH tätig. Sein Tätigkeitsschwerpunkt liegt auf der Einführung und Optimierung von Managementsystemen der deutschen Wäscherei- und Reinigungsbranche.

Daniel Dalkowski
Stellvertretender Geschäftsführer Deutscher Textilreinigungs-Verband



Daniel Dalkowski ist seit 2014 für den Deutschen Textilreinigungs-Verband tätig; seit 2021 als dessen stellvertretender Geschäftsführer. In dieser Funktion verantwortet er die Themen Kommunikation, Digitalisierung, Nachhaltigkeit und Personal. Zuvor studierte er an den Universitäten Marburg, Köln, Helsinki und Moskau und hat einen Master-Abschluss in Politikwissenschaft.

Hochschule Landshut
Prof. Dr. Matthias Dorfner



Prof. Dr. Dorfner verfügt über langjährige Erfahrung im Systems Engineering und ist als Professor an der Hochschule Landshut tätig. Er verfolgt einen ganzheitlichen Systems Engineering-Ansatz, um komplexe Wechselwirkungen entlang der Wertschöpfungskette zu analysieren und messbare Nachhaltigkeitsindikatoren zu definieren.

Hochschule Landshut
Prof. Dr. Sebastian Schröter



Prof. Dr. Schröter bringt umfangreiche Erfahrung im Systems Engineering mit und ist als Professor an der Hochschule Landshut tätig. Er setzt einen interdisziplinären Ansatz um, der komplexe Wechselwirkungen entlang der Wertschöpfungskette strukturiert analysiert und auf nachhaltige Lösungen fokussiert.

INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH
Lara Rosenthal (M.Eng.)



Lara Rosenthal verfasste ihre Masterarbeit bei der INTRASYS Beratungsgesellschaft für Unternehmensorganisation mbH im Rahmen des TEXSUS-Projekts. Seit knapp zwei Jahren ist sie dort als Unternehmensberaterin tätig und konzentriert sich auf die Umsetzung und Optimierung von Managementsystemen in der Wäschereibranche.

STEINHOFER Ingenieure GmbH
Dipl.-Ing. (FH) Bernd Steinhofer



Bernd Steinhofer ist Geschäftsführer-Gesellschafter der STEINHOFER Ingenieure GmbH, Regensburg. Das Ingenieur- und Beratungsunternehmen mit Schwerpunkt Sicherheitsplanung betreut und berät Kunden im gesamten Geschäftszyklus von der Gebäudekonzeption bis zum laufenden Geschäftsbetrieb.

KONTAKT

DTV
DEUTSCHER TEXTILREINIGUNGS-VERBAND
Daniel Dalkowski, Stellvertretender Geschäftsführer

Adenauerallee 48; 53113 Bonn
Tel.: +49 (0) 30 / 50 57 200 32
Mail: dalkowski@dtv-deutschland.de

INTRASYS
BERATUNGSGESELLSCHAFT FÜR UNTERNEHMENSORGANISATION MBH
Dipl. Betriebswirt (FH) Klaus Eder

Ludwig-Erhard-Straße 6; 84034 Landshut
Tel.: +49 (0) 871 / 96 28 41 0
Mail: klaus.eder@intrasys-gmbh.de

1 Vorwort: Warum Business Continuity Management und Brandschutz?

Sehr geehrte Leserinnen und Leser,

wir freuen uns, Ihnen unseren umfassenden Leitfaden zum Business Continuity Management und Brandschutz vorzustellen. Dieser Leitfaden ist ein unverzichtbares Werkzeug für Unternehmen. Business Continuity Management (BCM) und Brandschutz sind in der Wäschereibranche von besonderer Bedeutung, da der kontinuierliche Betrieb und die Sicherheit der Anlagen entscheidend für die Erfüllung der täglichen Aufträge sind. Wäschereien arbeiten häufig für zeitkritische Kunden wie Krankenhäuser, Pflegeeinrichtungen oder Hotels, bei denen ein Ausfall der Wäscheversorgung schnell schwerwiegende Folgen haben kann. Gleichzeitig ist der Produktionsprozess stark automatisiert und von funktionierenden Maschinen, Wasser-, Energie- und Chemikalienversorgung abhängig. Fällt eine dieser Komponenten aus, kommt der gesamte Betrieb rasch zum Stillstand. Besonders der Brandschutz spielt eine zentrale Rolle, da in Wäschereien durch Hitzeentwicklung in Trocknern und Mangeln, den Einsatz von Chemikalien sowie die große Menge an leicht brennbaren Textilien ein erhöhtes Brandrisiko besteht. Ein Brand hätte nicht nur personelle und materielle Schäden zur Folge, sondern könnte auch zu längeren Produktionsausfällen und dem Verlust wichtiger Kunden führen. Ein wirksames Business Continuity Management sorgt daher dafür, dass im Falle eines Brandes oder anderer Störungen geeignete Notfall- und Wiederanlaufpläne vorhanden sind, um den Betrieb so schnell wie möglich fortzusetzen. Somit tragen BCM und Brandschutz maßgeblich dazu bei, die Betriebssicherheit, Lieferfähigkeit und wirtschaftliche Stabilität eines Wäschereibetriebs langfristig zu sichern.

***Hinweis**: Für die meisten Wäscherei- und Textilreinigungsbetriebe ist die ISO 22301 in erster Linie als praxisorientierter Orientierungsrahmen zu verstehen; bereits mit den in diesem Leitfaden beschriebenen Grundmaßnahmen lässt sich ein Großteil des Nutzens eines BCM erzielen.*

1.1 Bedeutung der Geschäftskontinuität in einer systemrelevanten Branche

Die Wäscherei- und Textilreinigungsbranche ist ein unverzichtbarer Zulieferer für das Gesundheitswesen und weitere systemrelevante Bereiche. Als systemrelevante Branche trägt sie maßgeblich zur Aufrechterhaltung hygienischer Standards in Krankenhäusern, Pflegeeinrichtungen, der Lebensmittelindustrie und im Arbeitsschutz bei. Eine durchgängige Geschäftskontinuität ist daher unerlässlich – nicht nur zur Sicherung der eigenen Wirtschaftlichkeit, sondern auch im Interesse der öffentlichen Gesundheit und Sicherheit. Unternehmen sollten proaktiv Vorsorgemaßnahmen treffen, um auch in Krisensituationen handlungsfähig zu bleiben.

1.2 Auswirkungen von Betriebsunterbrechungen (z. B. Lieferausfälle im Gesundheitswesen)

Störungen im Wäschereibetrieb – etwa durch technische Defekte, Personalausfälle oder Naturkatastrophen – können gravierende Folgen haben. Besonders im Gesundheitswesen führen Lieferausfälle schnell zu hygienischen und medizinischen Versorgungsengpässen. Ohne regelmäßig aufbereitete

OP-Textilien, Pflegewäsche oder Schutzkleidung gerät die Betriebsfähigkeit medizinischer Einrichtungen in Gefahr. Auch in der Lebensmittelverarbeitung, Hotellerie und bei Rettungsdiensten entstehen rasch kritische Situationen.

Da Wäschereien systemrelevante Branchen beliefern, tragen sie in vielen Fällen eine Mitverantwortung innerhalb kritischer Infrastrukturen (KRITIS). Vor allem bei der Versorgung von Krankenhäusern, Pflegeheimen und Rettungsdiensten sind Ausfälle nicht nur betriebswirtschaftlich, sondern auch gesellschaftlich hoch relevant. Betriebsunterbrechungen beeinträchtigen somit nicht nur das eigene Unternehmen, sondern können ganze Versorgungsketten innerhalb der öffentlichen Daseinsvorsorge gefährden. Dies unterstreicht die Bedeutung eines professionellen Business Continuity Managements (BCM) mit klarem Fokus auf Resilienz und Reaktionsfähigkeit.

1.3 Gesetzliche und normative Anforderungen (ISO 22301, Arbeitsschutzgesetze, Brandschutzverordnungen)

Für das BCM selbst besteht keine unmittelbare gesetzliche Pflicht, wohl aber für zahlreiche seiner Bestandteile. Sie unterstützt Unternehmen dabei, Risiken zu identifizieren, Notfallpläne zu erstellen und betriebliche Resilienz aufzubauen.

Ergänzend gelten in Deutschland umfangreiche Arbeitsschutzgesetze und Brandschutzverordnungen, die betriebliche Sicherheitsstandards vorgeben – etwa zur Evakuierung, Brandvermeidung und zum Schutz von Beschäftigten. Die Einhaltung dieser Vorgaben ist nicht nur Pflicht, sondern ein wesentlicher Bestandteil nachhaltiger Unternehmensführung.

1.4 Einbettung in Nachhaltigkeitsstrategie und Risikomanagement

Die Geschäftskontinuität sollte integraler Bestandteil der Nachhaltigkeitsstrategie eines Unternehmens sein. Nachhaltigkeit umfasst nicht nur ökologische und soziale Aspekte, sondern auch wirtschaftliche Resilienz. Ein wirksames Risikomanagementsystem identifiziert potenzielle Störungen frühzeitig und ermöglicht strukturierte Prävention und Reaktion. Die Einbindung von Notfall- und Krisenmanagement in bestehende Managementsysteme – wie z. B. das Qualitäts- oder Umweltmanagement – stärkt die langfristige Unternehmensstabilität und schafft Vertrauen bei Mitarbeitenden, Kunden und Partnern. Besonders in der Wäschereibranche mit ihrer engen Verzahnung zu systemkritischen Einrichtungen ist dies von zentraler Bedeutung.

INHALT

1 Vorwort: Warum Business Continuity Management und Brandschutz? 6
1.1 Bedeutung der Geschäftskontinuität in einer systemrelevanten Branche 6
1.2 Auswirkungen von Betriebsunterbrechungen (z. B. Lieferausfälle im Gesundheitswesen) 6
1.3 Gesetzliche und normative Anforderungen (ISO 22301, Arbeitsschutzgesetze, Brandschutzverordnungen) 7
1.4 Einbettung in Nachhaltigkeitsstrategie und Risikomanagement 7
2 BCM in fünf Schritten für den Wäschereibetrieb 11
2.1 Schritt 1: Welche Prozesse dürfen, maximal 24 Stunden stillstehen? 11
2.2 Schritt 2: Wovon hängen diese Prozesse ab? 11
2.3 Schritt 3: Wer ruft wen an, wenn nachts etwas passiert? 12
2.4 Schritt 4: Wer übernimmt die Wäscheversorgung bei einem längeren Ausfall? 12
2.5 Schritt 5: Einmal im Jahr eine Stunde üben 13
3 Grundlagen 15
3.1 Definition und Ziele 15
3.1.1 Sicherstellung kritischer Geschäftsprozesse 15
3.1.2 Schutz von Menschen, Umwelt und Unternehmenswerten 16
3.2 Bezug zu Managementsystemen 16
3.2.1 Qualitäts-, Umwelt-, Energiemanagement 17
3.2.2 Verzahnung mit Arbeitssicherheits- und Brandschutzmanagement 17
4 Risikobewertung und Gefährdungsanalyse 18
4.1 Typische Risiken in der Branche 19
4.1.1 Brand, technische Störungen, Wasserschäden, Energieausfall, Lieferketteprobleme, Pandemien, Dampfkesselausfall 19
4.1.2 Cyberangriffe und IT-Ausfälle 20
4.2 BCM-Risikoanalyse 20
4.2.1 Business Impact Analysis (BIA) 20
4.2.2 Risiko-Matrix 21
4.3 Spezifische Brandschutzrisiken 23
4.3.1 Brandlasten in Wäschereien (Textilien, Verpackungen, Chemikalien) 23
4.3.2 Brandursachen (Maschinentechnik, Elektrik, Trockner, Lager) 23
5 Strategie und Maßnahmen 24
5.1 Präventionsmaßnahmen 24

5.1.1 Technischer Brandschutz (Brandmeldeanlagen, Löschanlagen, bauliche Trennung) 24
5.1.2 Organisatorischer Brandschutz (Brandschutzordnung, Unterweisung) 25
5.1.3 Redundanzen bei kritischen Prozessen (z.B. Zweitlieferanten, Ausweichproduktion) 26
5.1.4 IT-Sicherheit und Cyber-Resilienz 27
5.2 Notfallmaßnahmen 27
5.2.1 Räumungs-/ Evakuierungskonzepte 27
5.2.2 Alarmierungsketten 27
5.2.3 Erste-Hilfe und Feuerlöschtraining 28
5.2.4 IT-Notfallmanagement 28
5.3 Wiederanlaufstrategien 29
5.3.1 Priorisierung von Prozessen 29
5.3.2 Ersatzstandorte oder Partnerbetriebe 29
5.3.3 Verfügbarkeit von Textilbeständen 30
5.3.4 Kommunikation mit Kunden und Stakeholdern 30
6 BCM-Planung und -Dokumentation 31
6.1 Aufbau des BCM-Handbuchs 31
6.2 Notfall- und Krisenpläne 32
6.3 Brandschutzplan als integraler Bestandteil 32
6.4 Kontaktlisten und Ressourcenpläne 34
7 Schulungen, Training & Übungen 35
7.1 Regelmäßige Unterweisungen (inkl. Brandschutzübungen) 35
7.2 Simulation von Notfällen 36
7.3 Dokumentation der Übungen 36
8 Überprüfung & Verbesserung 37
8.1 Regelmäßige Audits 37
8.2 Auswertung von Vorfällen und Beinahe Ereignissen 37
8.3 Anpassung der Pläne an neue Risiken 38
8.4 Berücksichtigung von NIS-2 und KRITIS-Anforderungen 39
Anhänge (Formulare, Checklisten, Vorlagen) 41
Formular Checkliste Brandschutzprüfung 41
Formular Checkliste Evakuierungsplan 45
Formular Alarmierungs- und Notfallplan 49
Formular Notfall und Krisenplan – Chemieunfall 52
Formular Audits / Übung / Tests 55

Formular Audit & Verbesserung BCM 57
Formular Vorfallprotokoll inkl. Ursachenanalyse 59
Formular Kommunikationsplan im Krisenfall 62
Vorlage Vertretungsregelung bei Personalausfall 65

2 BCM in fünf Schritten für den Wäschereibetrieb

Viele Wäschereien verfügen bereits über ein gutes Qualitäts-, Hygiene-, Umwelt- oder Energiemanagement. Dennoch zeigt die Praxis, dass bereits ein einzelnes Ereignis den gesamten Betrieb zum Stillstand bringen kann.

Gerade Wäschereien versorgen oft Krankenhäuser, Pflegeeinrichtungen, Lebensmittelbetriebe oder andere Kunden mit hohen Anforderungen an Hygiene und Versorgungssicherheit. Ein Produktionsausfall kann daher weitreichende Folgen für Kunden, Mitarbeitende und das Unternehmen selbst haben. Business Continuity Management (BCM) hilft dabei, auf solche Situationen vorbereitet zu sein und den Betrieb schnellstmöglich wieder aufnehmen zu können. Es folgt eine kurze Zusammenfassung der fünf wichtigsten Schritte.

2.1 Schritt 1: Welche Prozesse dürfen, maximal 24 Stunden stillstehen?

Nicht alle Tätigkeiten sind gleich kritisch. Fragen Sie sich: **„Welche Prozesse müssen spätestens innerhalb von 24 Stunden wieder laufen?“**

Konzentrieren Sie sich zunächst auf die drei wichtigsten Prozesse. Wer alles als kritisch einstuft, priorisiert letztlich gar nichts.

Typische Beispiele:

- Bearbeitung von Krankenhauswäsche
- Tourenplanung
- Versorgung von Industriekunden

Notieren Sie für jeden Prozess:

Kritischer Prozess	Max. Ausfallzeit
…	….

2.2 Schritt 2: Wovon hängen diese Prozesse ab?

Sobald die kritischen Prozesse bekannt sind, wird analysiert, welche Ressourcen für deren Aufrechterhaltung benötigt werden. Fragen Sie sich: **„Was muss funktionieren, damit dieser Prozess läuft?“**

Mögliche Abhängigkeiten:

Infrastruktur

- Strom
- Gas
- Wasser
- ….

Personal

- Schichtleiter
- Techniker
- ....

Beispiel:

Prozess	Kritische Abhängigkeiten
Krankenhauswäsche	Dampf, Wasser, Tunnelwaschanlage, Dosieranlage
Tourenplanung	ERP-System, Internet, Disponent

Je besser die Abhängigkeiten bekannt sind, desto leichter lassen sich Risiken erkennen und vorbeugende Maßnahmen festlegen.

2.3 Schritt 3: Wer ruft wen an, wenn nachts etwas passiert?

Viele Unternehmen verfügen über technische Schutzmaßnahmen. Im Ernstfall scheitert die Reaktion jedoch oft an fehlender Kommunikation. Deshalb muss die **Alarmierungskette** klar definiert sein.

Stellen Sie sich immer folgende Fragen:

- Ist die Alarmierungskette schriftlich dokumentiert?
- Sind Mobilnummern aktuell?
- Gibt es Vertreterregelungen?
- Ist die Alarmierungskette ausgehängt?
- Wissen Mitarbeitende, wen sie anrufen müssen?

Die Alarmierungskette sollte mindestens einmal jährlich überprüft und aktualisiert werden.

2.4 Schritt 4: Wer übernimmt die Wäscheversorgung bei einem längeren Ausfall?

Die wichtigste BCM-Frage lautet: **„Wer hilft uns, wenn wir mehrere Tage oder Wochen nicht produzieren können?“**

Mögliche Lösungen:

Eigene Ersatzkapazitäten
Zweitstandort
Andere Niederlassung

Partnerbetriebe
Regionale Kooperationspartner
Andere Verbandsmitglieder

Stellen Sie sich auch hier im Vorhinein folgende Fragen:

- Wer unterstützt?
- Welche Kapazität steht zur Verfügung?
- Welche Wäschearten können übernommen werden?
- Wie erfolgt Transport und Abrechnung?
- Wer sind die Ansprechpartner?

Beistandsabkommen: Ein Beistandsabkommen sollte die gegenseitige Unterstützung im Falle einer Betriebsunterbrechung eindeutig regeln. Dabei sind insbesondere folgende Punkte festzulegen:

- ✓ **Verfügbare Kapazitäten und Reaktionszeiten** einschließlich Ansprechpartnern und Alarmierungswegen.
- ✓ **Hygieneanforderungen und Zertifizierungen** des Partnerbetriebes (z. B. RABC nach DIN EN 14065 sowie weitere relevante Zertifizierungen).
- ✓ **Technische Kompatibilität** der Prozesse und Systeme, insbesondere hinsichtlich RFID-/Chipsystemen, Textilarten, Waschprogrammen, Finishingprozessen und Sortierlogiken.
- ✓ **Logistische Abläufe**, einschließlich Zuständigkeiten für Transport, Abholung und Auslieferung.
- ✓ **Kaufmännische Regelungen** zu Preisen, Abrechnung, Haftung und Gewährleistung gegenüber dem Endkunden.
- ✓ **Datenschutz und Vertraulichkeit**, insbesondere bei der Verarbeitung von Kunden-, Mitarbeiter- oder Betriebsdaten.
- ✓ **Kartellrechtliche Vorgaben**, da es sich um eine Zusammenarbeit zwischen Wettbewerbern handelt und wettbewerbsbeschränkende Absprachen ausgeschlossen werden müssen.

Empfehlung: *Die Vereinbarung sollte regelmäßig überprüft und durch praktische Notfallübungen auf ihre Umsetzbarkeit getestet werden. Dadurch kann sichergestellt werden, dass die Zusammenarbeit im Ernstfall tatsächlich funktioniert.*

2.5 Schritt 5: Einmal im Jahr eine Stunde üben

Ein Notfallplan ist nur dann wirksam, wenn er getestet wird. Dazu genügt oft bereits eine einfache sogenannte Tischübung. Die Teilnehmer besprechen gemeinsam ein realistisches Szenario.

Beispiel-Szenario: Brand im Trocknerbereich um 22:00 Uhr

Fragen:

- Wer informiert wen?
- Welche Kunden sind betroffen?
- Wo werden Aufträge weiterbearbeitet?
- Welche Kommunikationswege werden genutzt?
- Welche Maschinen stehen weiterhin zur Verfügung?

Übungsprotokoll

Dokumentieren Sie:

- Datum
- Teilnehmer
- Szenario
- erkannte Schwachstellen
- vereinbarte Verbesserungsmaßnahmen
- Verantwortlichkeiten
- Termin zur Umsetzung

Empfehlung: (mindestens)

→ 1 Tischübung pro Jahr
→ 1 Überprüfung der Alarmierungskette pro Jahr
→ 1 Aktualisierung der Kontaktlisten pro Jahr
→ 1 Überprüfung der Beistandsvereinbarungen pro Jahr

3 Grundlagen

Das Business Continuity Management (BCM) ist ein systematischer Ansatz zur Erhaltung der Betriebsfähigkeit bei schwerwiegenden Störungen oder Krisen. Es verfolgt das Ziel, kritische Geschäftsprozesse auch in außergewöhnlichen Situationen aufrechtzuerhalten oder schnellstmöglich wiederherzustellen – sei es bei Naturereignissen, technischen Ausfällen, Pandemien oder Lieferengpässen.

In einer systemrelevanten Branche wie der Textilpflege ist BCM ein zentraler Bestandteil nachhaltiger Unternehmensführung und eng mit weiteren Managementsystemen wie Qualitäts-, Umwelt- oder Energiemanagement verbunden.

3.1 Definition und Ziele

BCM umfasst

- die strukturierte Vorbereitung auf potenzielle Bedrohungen,
- die Ermittlung von Risiken für die Betriebsabläufe sowie
- die Entwicklung von Strategien zur Krisenbewältigung und Wiederanlauf.

Ziel ist es, den Fortbestand des Unternehmens auch bei widrigen Bedingungen sicherzustellen – zum Schutz von Menschen, Umwelt und wirtschaftlichen Interessen.

3.1.1 Sicherstellung kritischer Geschäftsprozesse

In der Wäscherei- und Textilreinigungsbranche gelten insbesondere folgende Prozesse als kritisch für die Aufrechterhaltung des laufenden Betriebs und die Versorgung systemrelevanter Einrichtungen:

→ Annahme, Sortierung und Bearbeitung hygienerelevanter Textilien, insbesondere im Gesundheitswesen (z. B. Krankenhauswäsche, OP-Bekleidung, Bewohnerwäsche in Pflegeeinrichtungen), da diese unmittelbar mit dem Infektionsschutz und der Patientensicherheit verbunden sind.
→ Bereitstellung und termingerechte Lieferung von Miettextilien für medizinische, pflegerische sowie gewerbliche Einrichtungen – z. B. Schutzkleidung, Flachwäsche oder Mehrweg-OP-Textilien – stellt eine unverzichtbare Dienstleistung für den kontinuierlichen Betrieb dieser Einrichtungen dar.
→ Sicherstellung der Versorgungsinfrastruktur, insbesondere im Hinblick auf Energie (Strom, Dampf), Wasser und Personalressourcen, da Ausfälle in diesen Bereichen unmittelbar zu Produktionsunterbrechungen und Versorgungsengpässen führen können.

Unternehmen der Wäscherei- und Textilreinigungsbranche versorgen häufig Krankenhäuser, Pflegeeinrichtungen und weitere systemrelevante Einrichtungen. Dadurch können Anforderungen an Resilienz, Informationssicherheit und Notfallvorsorge für die Branche zunehmend an Bedeutung gewinnen. Auch wenn Wäschereibetriebe in der Regel nicht unmittelbar unter die gesetzlichen Anforderungen des KRITIS-Dachgesetzes oder der NIS-2-Regelungen fallen, ergeben sich entsprechende Erwartungen häufig über Kundenanforderungen, vertragliche Verpflichtungen, Ausschreibungen oder Lieferantenbewertungen.

Unternehmen sollten daher prüfen, welche Anforderungen sich aus ihren Kundenbeziehungen und Lieferketten ergeben, und angemessene organisatorische sowie technische Maßnahmen zur Sicherstellung ihrer Betriebs- und Lieferfähigkeit treffen.

3.1.2 Schutz von Menschen, Umwelt und Unternehmenswerten

Neben der Sicherung der Betriebsfähigkeit steht der Schutz von Beschäftigten und Umwelt im Mittelpunkt:

- Evakuierungs- und Alarmpläne bei Bränden oder Chemieunfällen
- Gesundheitsmaßnahmen bei pandemiebedingten Personalausfällen
- Schutz von Anlagen, Maschinen und IT-Systemen

BCM trägt damit zum Erhalt immaterieller Werte wie Reputation, Kundenzufriedenheit und Rechtssicherheit bei – und ist somit ein zentraler Bestandteil unternehmerischer Verantwortung (Corporate Responsibility).

3.2 Bezug zu Managementsystemen

BCM ist kein isoliertes System, sondern Teil eines integrierten Nachhaltigkeits- und Risikomanagements. In Wäschereien mit bestehenden ISO-Managementsystemen lässt sich BCM strukturiert andocken und effizient umsetzen.



BCM ist kein isoliertes System, sondern Teil eines integrierten Nachhaltigkeits- und Risikomanagements. In Wäschereien mit bestehenden ISO-Managementsystemen lässt sich BC strukturiert andocken und effizient umsetzen.

Das Business Continuity Management (BCM) steht in enger Verbindung mit dem Nachhaltigkeitsmanagement, den ISO-Managementsystemen und dem Risikomanagement. Während das Nachhaltigkeitsmanagement auf langfristige Stabilität und Verantwortung ausgerichtet ist, trägt das BCM dazu bei, diese durch Krisenfestigkeit und Lieferfähigkeit zu sichern. Die ISO-Managementsysteme, wie ISO 9001 (Qualität), ISO 14001 (Umwelt) oder ISO 27001 (Informationssicherheit), teilen mit der ISO 22301 (BCM) eine gemeinsame Struktur, was eine einfache Integration und Synergien in Risikoanalyse, Dokumentation und Verbesserung ermöglicht. Das Risikomanagement bildet dabei die Basis, indem es

Risiken identifiziert und bewertet, auf die das BCM mit konkreten Notfall- und Wiederanlaufmaßnahmen reagiert. Gemeinsam fördern diese Systeme eine nachhaltige, widerstandsfähige und verantwortungsvolle Unternehmensführung.

3.2.1 Qualitäts-, Umwelt-, Energiemanagement

Das Business Continuity Management (BCM) ergänzt bestehende Prozessbeschreibungen im Qualitätsmanagementsystem gezielt um Notfallprozesse und Wiederanlaufstrategien. Dadurch wird sichergestellt, dass auch bei Betriebsunterbrechungen – etwa durch technische Störungen, IT-Ausfälle oder Lieferengpässe – definierte Abläufe aufrechterhalten oder zeitnah wiederhergestellt werden können. BCM stärkt somit die Robustheit qualitätsrelevanter Kernprozesse und erhöht die Versorgungssicherheit gegenüber Kunden und Partnern.

Im Rahmen von Risiko- und Gefährdungsanalysen berücksichtigt das BCM auch umweltbezogene Störfälle und Notfallszenarien. Dazu zählen beispielsweise Havarien mit umweltgefährdenden Stoffen, Leckagen in Chemikalienlagern oder Störungen in der Abwasserbehandlung. Die Integration von Notfallplänen, Meldeketten und Schutzmaßnahmen in das Umweltmanagementsystem trägt zur Einhaltung gesetzlicher Pflichten sowie zur Vermeidung von Umweltschäden und Reputationsrisiken bei.

Der Ausfall kritischer Energieversorgungen – etwa von Strom, Dampf oder Prozesswärme – stellt ein zentrales Risiko für die Betriebskontinuität dar. BCM greift dieses Risiko auf und entwickelt präventive Maßnahmen wie Notstromversorgung, Spitzenlastmanagement oder Redundanzkonzepte in der Energieinfrastruktur. Durch diese Verzahnung entsteht ein belastbares Gesamtsystem, das sowohl auf Effizienz als auch auf Resilienz ausgelegt ist

3.2.2 Verzahnung mit Arbeitssicherheits- und Brandschutzmanagement

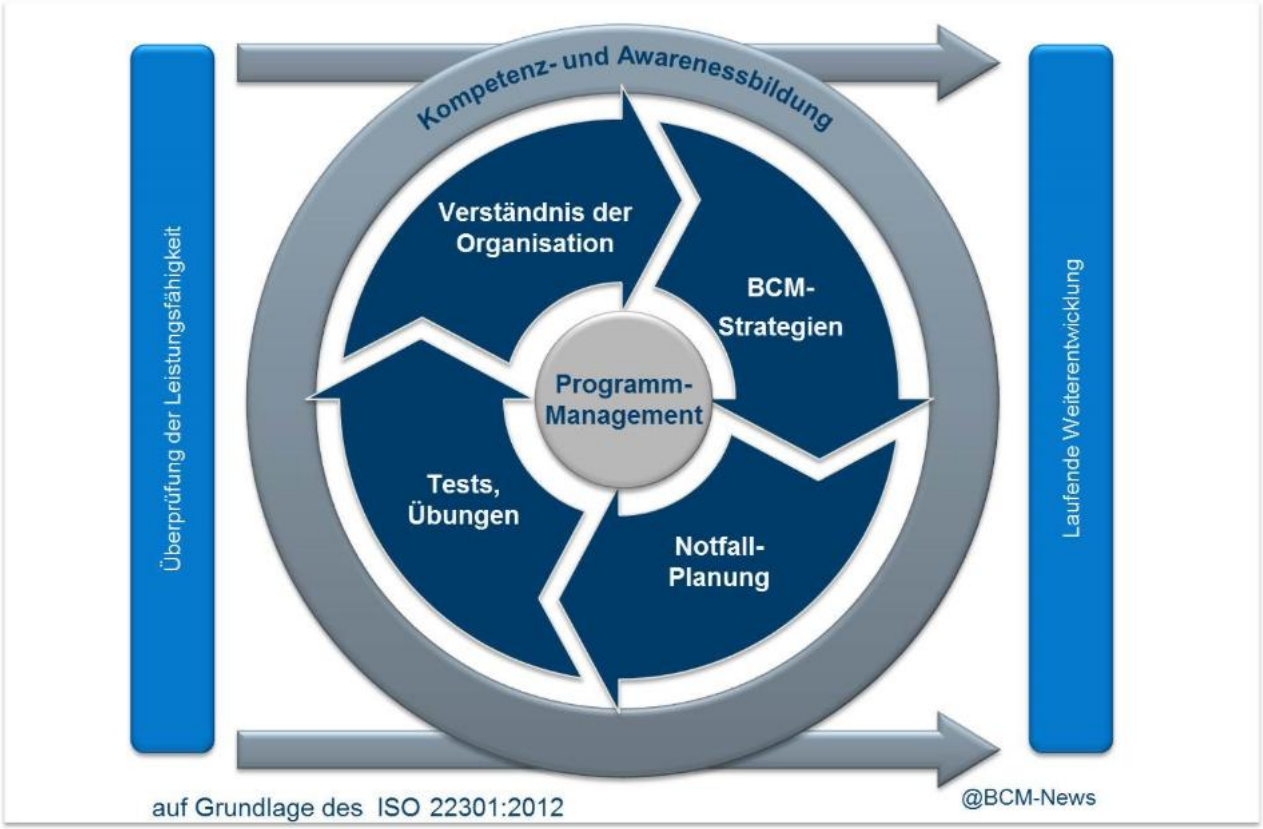
Das BCM baut auf bestehenden Sicherheits- und Präventionsmaßnahmen auf. Besonders wichtig sind dabei:

- Gefährdungsbeurteilungen nach dem Arbeitsschutzgesetz
- Brandschutzkonzepte nach landesspezifischen Gesetzen/ Bauordnungen
- Brandschutzordnungen gemäß DIN 14096 oder TRGS
- Evakuierungs- und Notfallübungen
- Kommunikationspläne für interne und externe Zielgruppen

Die Verzahnung mit bestehenden Systemen ermöglicht eine ganzheitliche Betrachtung von Risiken und verbessert die operative Resilienz – ohne Doppelarbeit.

4 Risikobewertung und Gefährdungsanalyse

Ein zentraler Bestandteil des Business Continuity Managements ist die systematische Erfassung und Bewertung von Risiken und Gefährdungen. Gerade in der energieintensiven und hochvernetzten Wäschereibranche sind Betriebe mit einer Vielzahl potenzieller Störfaktoren konfrontiert – von technischen Ausfällen über Versorgungsunterbrechungen bis hin zu externen Schocks wie Pandemien. Ziel der Risikobewertung ist es, relevante Bedrohungen zu identifizieren, ihre Auswirkungen einzuschätzen und darauf aufbauend geeignete Präventions- und Reaktionsmaßnahmen zu entwickeln.



4.1 Typische Risiken in der Branche

4.1.1 Brand, technische Störungen, Wasserschäden, Energieausfall, Lieferketteprobleme, Pandemien, Dampfkesselausfall

Brandrisiken:

Durch hohe Temperaturen, Wäschetrockner, chemische Stoffe und Flusenansammlungen besteht ein erhöhtes Brandentstehungsrisiko – besonders bei mangelndem Wartungs- oder Reinigungsturnus.

Technische Störungen:

Der Ausfall zentraler Maschinen wie Waschstraßen, Trockner oder Dosieranlagen kann zu erheblichen Produktionsunterbrechungen führen.

Energieausfälle:

Als energieintensive Branche sind Wäschereien stark abhängig von einer stabilen Energieversorgung. Stromausfälle oder Gasversorgungsengpässe wirken sich direkt auf Produktionsprozesse aus.

Wasserschäden:

Defekte Rohrleitungen, Überschwemmungen oder Rückstauereignisse gefährden nicht nur den Betrieb, sondern auch die Hygieneanforderungen.

Lieferkettenprobleme:

Verzögerungen bei der Anlieferung von Wasch- und Desinfektionsmitteln, Textilien oder Ersatzteilen können zu Stillständen führen – besonders bei Ein-Quellen-Beziehungen.

Pandemien / Personalausfälle:

Infektionswellen oder behördliche Quarantäneanordnungen führen zu akuten Personalengpässen. Auch Logistik und Kundenkontakte können massiv beeinträchtigt sein.

Ausfall Dampfkessel:

Der Ausfall der Dampferzeugung kann zu erheblichen Produktionsunterbrechungen führen, da zahlreiche Prozessschritte wie Waschen, Trocknen, Finishen und die Warmwasserbereitstellung von einer zuverlässigen Dampfversorgung abhängig sind.

All diese Risiken sollten systematisch in die betriebliche Risikoanalyse einfließen – idealerweise mit konkreten Szenarien und Notfallmaßnahmen.

4.1.2 Cyberangriffe und IT-Ausfälle

Die fortschreitende Digitalisierung der Wäscherei- und Textilreinigungsbranche erhöht die Abhängigkeit von informations- und kommunikationstechnischen Systemen. Produktionsanlagen, Dosieranlagen, ERP-Systeme, Tourenplanung, Kundenportale sowie digitale Zeiterfassung sind heute wesentliche Bestandteile der Betriebsabläufe.

Cyberangriffe, Schadsoftware (z. B. Ransomware), Serverausfälle oder der Ausfall von Cloud-Diensten können innerhalb kurzer Zeit zu erheblichen Betriebsunterbrechungen führen. Neben Produktionsausfällen drohen Datenverlust, Kommunikationsprobleme sowie erhebliche wirtschaftliche Schäden.

Daher sollten Cyberrisiken als eigenständiger Bestandteil der BCM-Risikoanalyse bewertet und mit geeigneten Präventions- und Wiederanlaufmaßnahmen berücksichtigt werden.

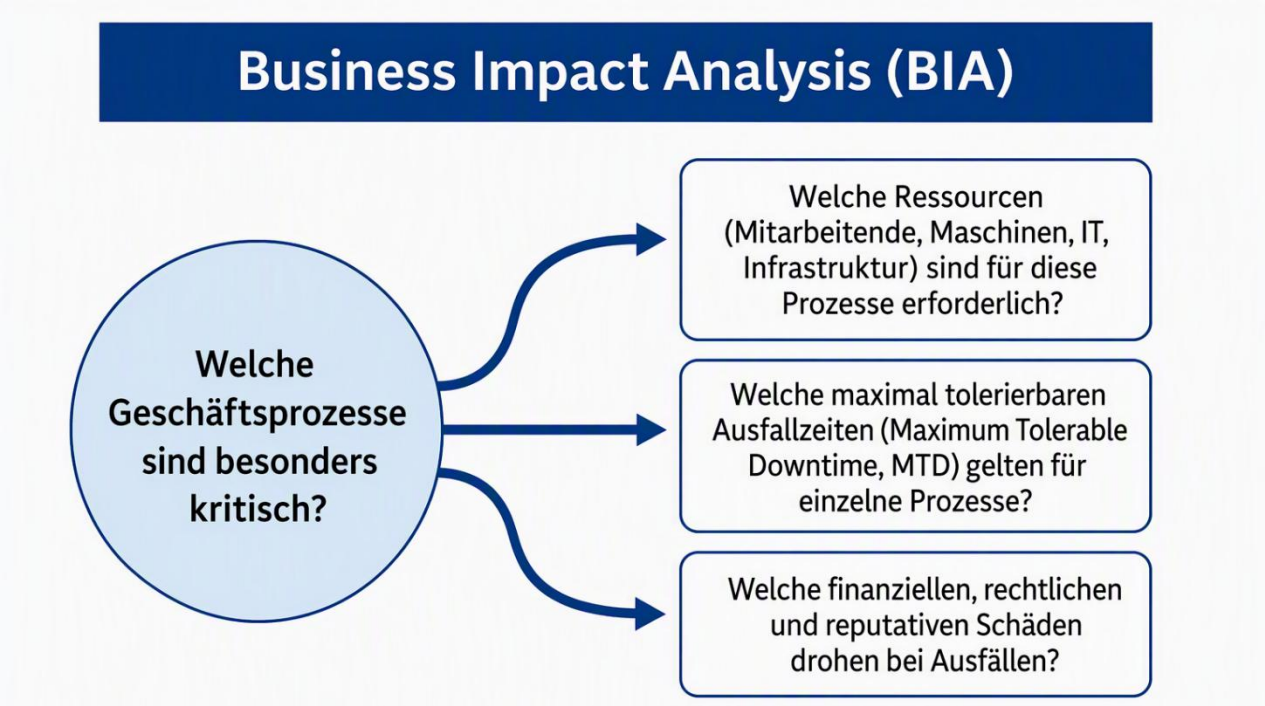
4.2 BCM-Risikoanalyse

Zwei bewährte Methoden für die strukturierte Analyse und Bewertung von Risiken im Kontext von BCM sind die Business Impact Analysis (BIA) und die Risikomatrix.

4.2.1 Business Impact Analysis (BIA)

Die **Business Impact Analysis (BIA)** ist ein zentrales Instrument zur Bewertung der Auswirkungen potenzieller Störungen auf den Geschäftsbetrieb. Ziel ist es, folgende Fragen zu beantworten:

- Welche Geschäftsprozesse sind besonders kritisch?
- Welche Ressourcen (Mitarbeitende, Maschinen, IT, Infrastruktur) sind für diese Prozesse erforderlich?
- Welche maximal tolerierbaren Ausfallzeiten (Maximum Tolerable Downtime, MTD) gelten für einzelne Prozesse?
- Welche finanziellen, rechtlichen und reputativen Schäden drohen bei Ausfällen?



Hinweis: Diese Grafik wurde mit Hilfe von KI erstellt

In der Wäschereibranche betrifft dies typischerweise Prozesse wie die Hygienewäsche für das Gesundheitswesen, die Logistik für OP-Textilien oder die Versorgung mit Mietberufskleidung. Die BIA liefert die Grundlage für die Entwicklung zielgerichteter Notfallmaßnahmen und Wiederanlaufstrategien.

Im Rahmen der Business Impact Analysis sollten auch informations- und kommunikationstechnische Ressourcen bewertet werden. Hierzu gehören insbesondere:

- ERP-Systeme
- Produktionssteuerungen
- Tourenplanung
- Dokumentenmanagement
- Labor- und Dosiersysteme
- Kommunikationssysteme
- Cloud-Dienste

Für diese Systeme sind maximale Ausfallzeiten sowie Wiederherstellungsprioritäten festzulegen. Die Ergebnisse bilden die Grundlage für das IT-Notfallmanagement.

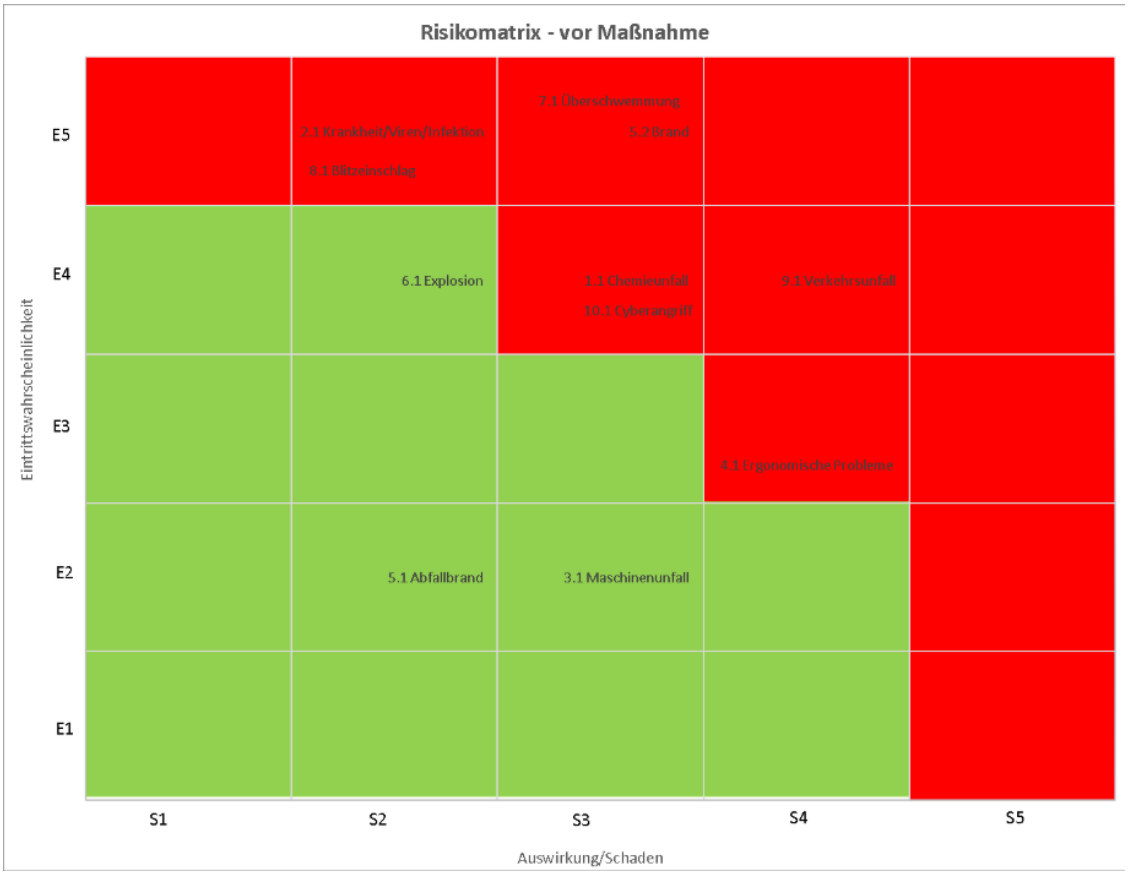
4.2.2 Risiko-Matrix

Die **Risikomatrix** ist ein bewährtes Instrument zur grafischen Bewertung von Risiken nach zwei Kriterien:

- **Eintrittswahrscheinlichkeit** (z. B. häufig, gelegentlich, selten)
- **Auswirkung auf den Betrieb** (z. B. gering, mittel, kritisch, existenzbedrohend)

Typischerweise wird daraus eine 3x3- oder 5x5-Matrix erstellt, in der Risiken visuell zugeordnet werden können. Risiken mit hoher Eintrittswahrscheinlichkeit und kritischen Auswirkungen (z. B. Maschinenbrand oder IT-Ausfall) sind prioritär zu behandeln, während seltene Risiken mit geringen Auswirkungen dokumentiert, aber nicht sofort adressiert werden müssen.

So könnte eine Risikomatrix aussehen, die sich aus einer Risikoanalyse ergibt. (Die Nummern ergeben sich aus interner Kennzeichnung der Risiken)



Die Einstufung der Schadenshöhe könnte wie folgt aussehen:

Definition Schadenhöhe

Wert	Festlegung	Klassifizierung
S 1	Vorfalll verursacht geringe Schäden	Keine Beeinträchtigung der relevanten Geschäftsprozesse und Tätigkeiten
S 2	Vorfall verursacht mittlere Schäden	mögliche leichte reversible Beeinträchtigung von Prozessen, Fehlfunktionen
S 3	Vorfall verursacht beträchtliche Schäden	mögliche reversible Beeinträchtigung von Prozessen, Fehlfunktionen
S 4	Vorfall verursacht hohe Schäden	mögliche schwere Schäden von Prozessen, Mitarbeitern
S 5	Vorfall verursacht extrem hohe Schäden	Bleibende schwerwiegene Schäden an Mitarbeitern, Prozessen

Grenzwerte Einzelrisiken

	Von	Bis
Vertretbarer Bereich	1	4
Unvertretbarer Bereich	5	5

4.3 Spezifische Brandschutzrisiken

4.3.1 Brandlasten in Wäschereien (Textilien, Verpackungen, Chemikalien)

Brandlasten liegen in Wäschereien in vielfältigen Ausprägungen vor. Dabei stellen vor allem die großen Mengen an Textilien aus Natur- und Kunstfaserstoffen den Hauptanteil dar. Mit den Textilien sowie den im Reinigungsprozess entstehenden Nebenprodukten aus Flusen und der gleichen liefern diese erhöhten Brandlasten die Grundlage eines erhöhten Brandentstehungsrisikos.
Daneben bedingen die Produktionsprozesse und -verfahren auch den Einsatz von Chemikalien und sonstigen (leicht) entzündlichen oder Brand fördernden Stoffen, die bei unsachgemäßer Lagerung oder Handhabung die Brandausbreitung begünstigen.

4.3.2 Brandursachen (Maschinentechnik, Elektrik, Trockner, Lager)

Nachdem für eine Brandentstehung generell drei Parameter erforderlich sind, nämlich

- brennbarer Stoff/ Brandlast
- Energie/ Zündquelle und
- Sauerstoff

ergeben sich dadurch verschiedenartige Brandentstehungsursachen.

Im Produktionsablauf am Anfang steht die Wäscheanlieferung, bei der nicht auszuschließen ist, dass „schwarze“ Wäsche durch den Einsatz beim Kunden mit Ölen, Fetten oder sonstige Mitteln aus medizinischen Anwendungen oder dergleichen verschmutzt sind. Die durch die Kompression der Wäsche in den Wäschesäcken entstehende Energie in Verbindung mit der Brand fördernden Brandlast aus Textilien und chemischen Stoffen kann eine Brandentstehung begünstigen.

Im Weiteren stellen Verunreinigungen durch Flusen auf heißen Oberflächen der Produktionsanlagen die Grundlage der Brandentstehung dar.

Auch im Warenlager und der -kommissionierung kann es durch „weiße“ Wäsche, die warm/ heiß gestapelt wird, zu einer Brandentstehung kommen.

Ergänzt werden diese Branchenspezifischen Brandursachen durch die allgemein in Deutschland verbreiteten Brandursachen wie technische Defekte von Maschinen/ Elektrizität (ca. 30% gem. Brandursachenermittlungen des IFS) und Fehlverhalten von Menschen (ca. 22%).

5 Strategie und Maßnahmen

5.1 Präventionsmaßnahmen

5.1.1 Technischer Brandschutz (Brandmeldeanlagen, Löschanlagen, bauliche Trennung)

Als präventive Maßnahmen vereint der Technische Brandschutz bautechnische und anlagentechnische Komponenten, die dem sogenannten vorbeugenden Brandschutz zuzuordnen sind. Die sinnvolle Kombination verschiedener Einzelkomponenten trägt dazu bei die definierten Schutzziele zu erreichen. Dabei ist es von Bedeutung, neben dem öffentlichen-rechtlichen Schutzzielen aus den Bauordnungen und Gesetzen, die für einen ordnungsgemäßen Betrieb zwingende Voraussetzung sind, auch die Anforderungen aus den Vorgaben des Sachversicherers im Blick zu behalten.

So sorgen bauliche Maßnahmen, wie Brandwände oder weitergehende brandschutztechnisch wirksame Trennwände mit den zugehörigen Brandschutztüren dafür, dass sich Brand und Rauch auf definierte Bereiche begrenzen lassen und somit auch ein Brandereignis wirksam von den Feuerwehren bekämpft werden kann. Je kleinteiliger diese Trennungen sein können, je weniger Betriebsausfall ist zu erwarten.

Neben diesen baulichen Maßnahmen können Brandschutzanlagen dabei helfen, ein Brandereignis frühzeitig zu entdecken (Brandmeldeanlage) oder auch mit den verschiedenartigen Löschanlagen das Brandereignis zu begrenzen und „in Schach“ zu halten, bis die Feuerwehr kommt. Beide Komponenten werden zumeist bei den Baumaßnahmen der Produktionsanlagen geplant und umgesetzt. Die Herausforderung im täglichen Betrieb besteht dann darin, diesen Technischen Brandschutz durch regelmäßige Prüfung und Wartung auf Stand zu halten, sodass er betriebssicher und wirksam funktioniert, aber ihn auch nicht außer Kraft zu setzen durch z.B. unzulässiges Aufkeilen von Brandschutztüren.



Technischer Brandschutz – richtig geplant, umgesetzt und aufrechterhalten – ist die Basis, bei einem Brandereignis möglichst wenig Betriebsausfall und -unterbrechung zu haben, ganz abgesehen davon, dass Personenschaden als oberstes Schutzziel vermieden wird.

5.1.2 Organisatorischer Brandschutz (Brandschutzordnung, Unterweisung)

Die Maßnahmen des organisatorischen Brandschutzes sind ein zentraler Bestandteil des vorbeugenden Brandschutzes und zielen darauf ab, durch strukturierte Abläufe, Verantwortlichkeiten und Schulungen Brände zu verhindern, Brandausbreitung zu begrenzen und im Brandfall schnelle, koordinierte Reaktionen zu ermöglichen. Sie ergänzen die baulichen und technischen Schutzmaßnahmen und sind unabhängig von der Gebäudeart in jedem Betrieb relevant – besonders in sensiblen Branchen wie Wäschereien und Textilreinigungen, in denen mit brennbaren Stoffen, elektrischen Anlagen, Chemikalien und thermischen Prozessen gearbeitet wird.

Organisatorische Maßnahmen sind:

Festlegung von Verantwortlichkeiten
• **Brandschutzbeauftragte**: Bestellung und Benennung einer fachlich geschulten Person, die den Brandschutz koordiniert, kontrolliert und dokumentiert. • **Brandschutzhelfer**: Ausgebildete Mitarbeitende, die im Notfall Löschversuche unternehmen oder die Evakuierung unterstützen. • Zuständigkeiten im Notfall: Wer alarmiert? Wer führt an? Wer betreut Gäste, Kunden, Einsatzkräfte?
Brandschutzordnung (nach DIN 14096, Teile A–C)
• Teil A: Kurzinformation für alle Personen im Gebäude – z. B. aushängend im Eingangsbereich. • Teil B: Verhaltensregeln für alle Beschäftigten (z. B. bei Brandentdeckung, Räumung). • Teil C: Detaillierte Regelungen für Personen mit besonderen Aufgaben im Brandschutz.
Unterweisung und Schulung
• Regelmäßige Unterweisungen (mind. jährlich) aller Beschäftigten zum richtigen Verhalten im Brandfall und zu Brandschutzvorgaben. • Schulung von Brandschutzhelfern (gemäß ASR A2.2) inkl. Handhabung von Feuerlöschern. • Einweisung von Fremdfirmen (z. B. Techniker, Reinigungskräfte) in brandschutzrelevante Regeln.
Evakuierungs- und Alarmierungsmanagement
• Erstellung und Kommunikation eines Räumungsplans, inklusive Notausgängen, Sammelstellen und alternativer Wege. • Durchführung von Räumungsübungen, idealerweise jährlich. • Festlegung der internen Alarmierungskette – wer informiert wen, wann und wie?
Betriebsorganisation und Gefährdungsbeurteilung
• Risikobewertung aller Arbeitsbereiche hinsichtlich Brandgefahr (z. B. Wäschereibereich, Chemielager, Maschinenräume). • Definition sicherer Lager- und Arbeitsbereiche: z. B. keine Lagerung brennbarer Stoffe im Fluchtweg. • Sicherer Umgang mit Arbeitsmitteln (z. B. Trockner, Mangeln, Reinigungsanlagen). • Verhaltensregeln für bestimmte Tätigkeiten wie Heißarbeiten, Wartungen, Abschaltungen.

Zutritts- und Zugangskontrollen
• Zutrittsbeschränkungen zu gefährdeten Bereichen (z. B. Chemikalienlager, Maschinenräume). • Freihaltung von Flucht- und Rettungswegen sowie der Feuerwehrzufahrten.
Löschmittelmanagement
• Standorte und Funktionstüchtigkeit von Feuerlöschern regelmäßig prüfen und dokumentieren. • Sichtprüfung und Wartung durch Sachkundige (gem. DIN 14406-4). • Löschdecken, Wandhydranten oder automatische Systeme betriebsbereit halten.
Dokumentation und Kontrolle
• Führen eines Brandschutzakte (z. B. mit Genehmigungen, Prüfprotokollen, Wartungen, Schulungsnachweisen). • Regelmäßige Begehungen durch Brandschutzbeauftragte und Fachkräfte für Arbeitssicherheit. • Maßnahmen aus Begehungen, Prüfungen oder Beinahe-Ereignissen nachvollziehbar dokumentieren.
Zusammenarbeit mit Behörden & Feuerwehr
• Erstellung von Feuerwehrplänen (z. B. für Sonderbauten, Wäschereien mit KRITIS-Relevanz). • Abstimmung der Evakuierungskonzepte mit der Feuerwehr. • Teilnahme an gemeinsamen Übungen oder Schulungen.
Besondere Regelungen für sensible Bereiche
• Umgang mit Chemikalien (Lagerung, Trennung, Kennzeichnung, Sicherheitsdatenblätter). • Wartung und Überwachung elektrischer Anlagen – z. B. Prüfungen nach DGUV Vorschrift 3. • Besondere Vorsicht bei heißen Maschinen und Wäscheaufbereitung (z. B. Glimmnester in Trocknern → Risiko Spontanentzündung).

5.1.3 Redundanzen bei kritischen Prozessen (z.B. Zweitlieferanten, Ausweichproduktion)

Im Rahmen des BCM sollte sich jeder Verantwortliche in einem Unternehmen bewusst machen, dass ein Brand jederzeit entstehen kann und das Brandereignis zu einer Betriebsunterbrechung führen kann. Je besser oben genannte Präventionsmaßnahmen geplant, umgesetzt und gelebt werden, kann davon ausgegangen werden, dass sich betroffene Bereiche eingrenzen lassen. Dennoch wird es dazu führen, dass die Produktion für eine gewisse Zeit ausfallen kann. Auch sollte sich im Rahmen des BCM jeder Verantwortliche bewusst sein, dass dies auch jederzeit bei einem Lieferanten möglich ist.

Somit muss es das Ziel eines nachhaltigen Produktionsprozesses sein, Risiken zu identifizieren und Alternativen vorzusehen.

5.1.4 IT-Sicherheit und Cyber-Resilienz

Cyber-Resilienz beschreibt die Fähigkeit eines Unternehmens, trotz Cyberangriffen oder IT-Störungen den Geschäftsbetrieb aufrechtzuerhalten oder möglichst schnell wiederherzustellen.

Grundlage hierfür sind technische und organisatorische Sicherheitsmaßnahmen wie:

- regelmäßige Datensicherungen,
- mehrstufige Zugriffskonzepte,
- Mehr-Faktor-Authentifizierung,
- Netzwerksegmentierung,
- Patch- und Update-Management,
- Virenschutz- und Endpoint-Security,
- Überwachung kritischer Systeme,
- Schulung der Mitarbeitenden zur Erkennung von Phishing-Angriffen.

Cyber-Resilienz ergänzt die klassischen Maßnahmen des Business Continuity Managements und trägt wesentlich zur Sicherstellung der Geschäftskontinuität bei.

5.2 Notfallmaßnahmen

5.2.1 Räumungs-/ Evakuierungskonzepte

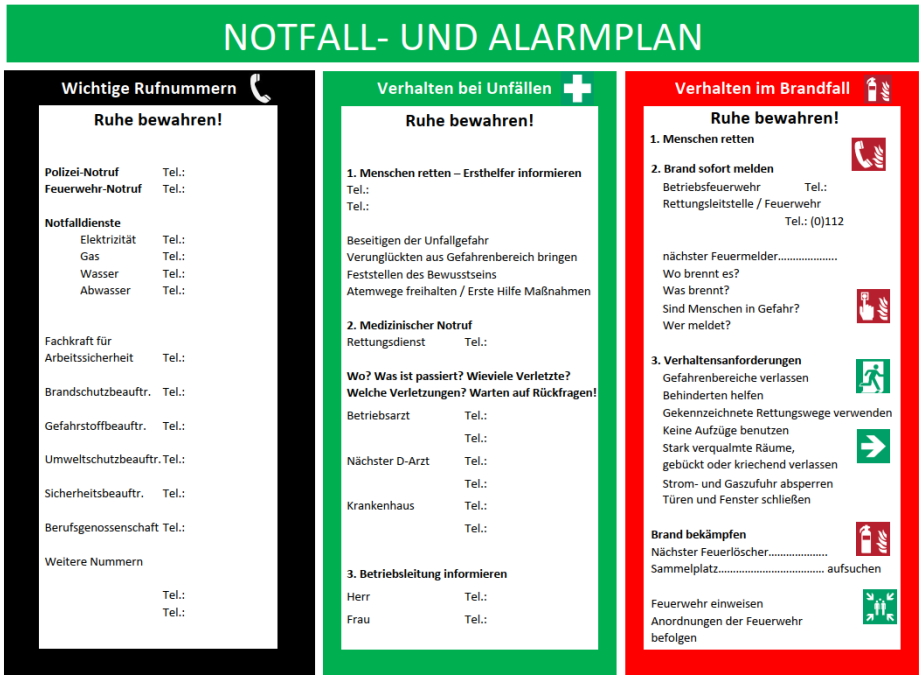
Neben der Tatsache, dass Menschenleben das höchste und unverhandelbare Schutzziel im Brandschutz ist, muss im Sinne der Betriebsaufrechterhaltung auch Sorge dafür getragen werden, dass bei einem Brandereignis die Personen im Objekt auf schnellsten, kürzesten und sichersten Weg das Objekt verlassen können.

Strukturierte Räumungs-/ Evakuierungskonzepte berücksichtigen dabei immer, dass es für die Produktionsbereiche zwei voneinander unabhängige Möglichkeiten gibt, über die sich die Mitarbeitenden selbst aus dem Gebäude retten können. Visuell können diese Räumungs-/ Evakuierungskonzepte den Personen im Objekt durch Flucht- und Rettungspläne in ausreichender Anzahl und Verteilung nähergebracht werden.

Die Praxis hierbei zeigt aber auch, dass nur Konzepte dann ihre Wirkung entfalten können, wenn eine Routine durch regelmäßige Übungen entsteht.

5.2.2 Alarmierungsketten

Es brennt und nichts passiert. Mangelnde Information, Kommunikation und Organisation lassen Technische Brandschutzmaßnahmen unwirksam erscheinen.
Daher ist es entscheidend, dass im Rahmen der Ablauforganisation definiert wird, welche Schritte wer erledigt, wenn ein Brandereignis auftritt. Beginnend bei jedem Mitarbeitenden, der ein Brandereignis entdeckt und hieraus die Kollegen warnt und informiert, das Gebäude auf den vorgegebenen Wegen zu verlassen, muss diese Information auch an die maßgebenden Stellen im Unternehmen ankommen, die weitergehende Maßnahmen ergreifen.



Weiterführende Infos/ Tools:

- Formular Alarmierungskette im Notfall
- Alarmplan, Stand: 01/2018

5.2.3 Erste-Hilfe und Feuerlöschtraining

Werden Brände im Stadium eines Entstehungsbrandes entdeckt, ist es einem geschulten Mitarbeitenden durchaus möglich, diesen mit den vorhandenen Selbsthilfeeinrichtungen/ Feuerlöschern zu bekämpfen und somit ein ausgedehntes Brandereignis zu vermeiden. Mit Hilfe von Brandschutzschulungen und Feuerlöscher-Trainings werden die Grundlagen des BCM gelegt, sodass es gar nicht zu einem weitgreifenden Ausfall kommt.

5.2.4 IT-Notfallmanagement

Das IT-Notfallmanagement beschreibt alle Maßnahmen zur schnellen Wiederherstellung informations- und kommunikationstechnischer Systeme nach einem Ausfall oder Cyberangriff.
Bestandteil eines IT-Notfallplans sind insbesondere:

- Alarmierungswege,
- Verantwortlichkeiten,
- Wiederherstellung von Backups,
- Notfallarbeitsplätze,
- Ersatzhardware,
- Kommunikation mit IT-Dienstleistern,
- Dokumentation des Vorfalls,
- Wiederinbetriebnahme der Systeme.

Der IT-Notfallplan sollte regelmäßig getestet und mit den allgemeinen BCM-Notfallplänen abgestimmt werden.

5.3 Wiederanlaufstrategien

Wiederanlaufstrategien beschreiben, wie ein Unternehmen nach einer Betriebsunterbrechung seine kritischen Prozesse zeitnah, koordiniert und mit möglichst geringen Schäden wieder aufnehmen kann. Sie sind ein zentrales Element des Business Continuity Managements (BCM) und müssen sowohl technische, personelle als auch logistische Aspekte berücksichtigen. Ziel ist es, die Versorgungssicherheit – insbesondere für systemrelevante Kunden – zu gewährleisten und wirtschaftliche Verluste zu minimieren.

5.3.1 Priorisierung von Prozessen

Im Krisenfall steht nicht immer die volle Kapazität oder Infrastruktur zur Verfügung. Daher ist es notwendig, bereits im Vorfeld eine klare Priorisierung der Geschäftsprozesse vorzunehmen. Dies erfolgt auf Basis ihrer Kritikalität und Auswirkungen bei Ausfall.
Für die Wäscherei- und Textilreinigungsbranche bedeutet das beispielsweise:

- **Höchste Priorität**: Bearbeitung und Lieferung hygienerelevanter Textilien (z. B. Krankenhaus- und Pflegewäsche), da deren Ausfall unmittelbar die Patientensicherheit gefährdet.
- **Mittlere Priorität**: Versorgung gewerblicher Kunden mit hoher Abhängigkeit (z. B. Lebensmittelindustrie, Reinraumbetriebe).
- **Niedrigere Priorität**: Servicebereiche, administrative Tätigkeiten oder Textilien mit längeren Lieferfristen.

Die Priorisierung erfolgt idealerweise anhand einer **BCM-Risikoanalyse** und ist regelmäßig zu überprüfen. Sie bildet die Grundlage für die Ressourcenzuteilung im Wiederanlauf (z. B. Personal, Energie, Maschinenverfügbarkeit).

5.3.2 Ersatzstandorte oder Partnerbetriebe

Ein wesentlicher Bestandteil der Wiederanlaufstrategie ist die Festlegung von Ersatzkapazitäten für den Fall, dass der Hauptstandort ganz oder teilweise ausfällt. Hierzu zählen:

→ Interne Alternativen (sofern vorhanden): Zweigbetriebe oder andere Standorte des Unternehmens.
→ Kooperation mit Partnerbetrieben: Gemeinsame Notfallabsprachen (Beistandsabkommen) innerhalb eines Netzwerks (z. B. regionaler Wäschereizusammenschlüsse, Verbandsmitglieder im DTV).
→ Externe Dienstleister: Vorverhandelte Rahmenverträge mit verlässlichen Dienstleistern, die im Bedarfsfall temporäre Produktions- oder Logistikleistungen übernehmen.

Wichtig ist, dass Kapazitäten, Hygieneanforderungen, Zertifizierungen und Lieferwege im Vorfeld abgestimmt sind.

Für kritische IT-Systeme sind Wiederherstellungsziele festzulegen. Hierzu gehören insbesondere die maximal zulässige Ausfallzeit (Recovery Time Objective – RTO) sowie der maximal tolerierbare Datenverlust (Recovery Point Objective – RPO). Diese Zielgrößen unterstützen die Priorisierung der Wiederanlaufmaßnahmen und ermöglichen eine strukturierte Wiederherstellung der Geschäftsprozesse.

5.3.3 Verfügbarkeit von Textilbeständen

Neben Produktionskapazitäten und Personalressourcen ist auch die Verfügbarkeit von Textilien für den Wiederanlauf von entscheidender Bedeutung. Insbesondere in Mietwäschebetrieben stellt der Textilbestand häufig das größte Umlaufvermögen des Unternehmens dar. Nach einem Brand- oder Schadensereignis können Textilien durch Feuer-, Rauch- oder Löschwasserschäden ganz oder teilweise ausfallen. Besonders kritisch sind kundenspezifische Artikel wie Berufskleidung mit Firmenlogo, Namenskennzeichnung, RFID-Transpondern oder individuellen Ausstattungsmerkmalen, da deren Wiederbeschaffung und Aufbereitung oftmals mehrere Wochen oder Monate in Anspruch nimmt. Unternehmen sollten daher kritische Textilbestände identifizieren, Wiederbeschaffungszeiten bewerten und geeignete Vorsorgemaßnahmen, beispielsweise Sicherheitsbestände oder alternative Beschaffungsmöglichkeiten, festlegen.

5.3.4 Kommunikation mit Kunden und Stakeholdern

Transparente, zeitnahe und strukturierte Kommunikation ist im Krisenfall entscheidend, um Vertrauen zu erhalten, Eskalationen zu vermeiden und gemeinsam mit Kunden tragfähige Lösungen zu finden. Daher sollten Unternehmen bereits im Vorfeld Kommunikationsstrategien und -wege definieren.

Elemente der Notfallkommunikation:

- Erstellung eines Kommunikationsplans mit Zuständigkeiten, Textbausteinen und Kontaktlisten.
- Frühzeitige Information kritischer Kunden bei drohenden oder eingetretenen Versorgungsengpässen.
- Proaktive Kommunikation mit Behörden, Gesundheitsämtern oder Aufsichtsstellen, falls die Versorgung von KRITIS-Einrichtungen betroffen ist.
- Regelmäßige Updates zum Wiederanlaufstatus, idealerweise über persönliche Ansprechpartner oder digitale Kanäle.

Auch interne Kommunikation spielt eine zentrale Rolle: Mitarbeitende müssen wissen, wann und wie sie im Krisenfall reagieren, wen sie informieren und welche Aufgaben sie übernehmen sollen.

Weiterführende Infos/ Tools:

- Formular Kommunikationsplan im Krisenfall

6 BCM-Planung und -Dokumentation

Ein wirksames Business Continuity Management (BCM) lebt nicht nur von der Analyse von Risiken, sondern vor allem von der konkreten Planung und systematischen Dokumentation. Die Erstellung eines BCM-Handbuchs, klar strukturierter Notfall- und Krisenpläne sowie ergänzender Dokumente wie Kontaktlisten und Ressourcenübersichten ist essenziell, um im Ernstfall schnell und zielgerichtet handeln zu können.

Gesetzliche und normative Grundlagen:

- ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements
- Arbeitsschutzgesetz (ArbSchG)
- Muster-Industriebaurichtlinie (MIndBauRL)
- Brandschutzverordnungen der Länder
- DGUV Vorschrift 1 – Grundsätze der Prävention
- TRGS 800 – Maßnahmen gegen Brände und Explosionen bei Tätigkeiten mit Gefahrstoffen

6.1 Aufbau des BCM-Handbuchs

Das BCM-Handbuch bildet die zentrale Dokumentation aller Maßnahmen zur Sicherstellung der Geschäftskontinuität. Es sollte klar strukturiert, verständlich formuliert und regelmäßig aktualisiert sein.

Der Aufbau kann sich an folgenden Kapiteln orientieren:

1. Einleitung und Geltungsbereich
2. Verantwortlichkeiten und Ansprechpartner (inkl. Vertretungsregelungen)
3. Ergebnisse der Business Impact Analyse (BIA)
4. Risikobewertung und -klassifizierung
5. Notfall- und Wiederanlaufpläne (Recovery Plan)
6. Kommunikationsstrategie (intern/extern)
7. Schulungs- und Übungspläne
8. Verweise auf weitere relevante Pläne (z. B. Brandschutz, IT-Sicherheit, Pandemieplan)

Tipp: Im Rahmen von ISO 22301 kann das BCM-Handbuch als integraler Bestandteil eines umfassenden Managementsystems aufgebaut sein, das sich mit ISO 9001, ISO 14001 oder ISO 45001 verzahnt.

6.2 Notfall- und Krisenpläne

Notfall- und Krisenpläne beschreiben Schritt-für-Schritt-Abläufe für verschiedene Schadens- und Störungsszenarien. Sie helfen, in Stresssituationen systematisch und effizient zu reagieren und Schäden zu minimieren.

Beispielhafte Inhalte:

- Szenariobeschreibungen (z. B. Brand, Stromausfall, Lieferkettenunterbrechung, Wasserschaden, Cyberangriff, Ransomware, Ausfall des ERP-Systems, Ausfall der Produktionssteuerung, Ausfall der Telefonie, Cloud-Ausfall)
- Alarmauslösung und Erstreaktion
- Evakuierungswege und Sammelstellen
- Verantwortlichkeiten im Krisenstab
- Kommunikationswege (z. B. Info an Kunden, Behörden, Presse)
- Wiederanlaufmaßnahmen und Alternativen

TEXSUS empfiehlt die Ausarbeitung von branchenangepassten Notfallplänen, z. B. für OP-Wäschelogistik, Chemieunfall in der Dosieranlage oder Ausfall des Trocknerparks

Weiterführende Infos/ Tools:

- Formular Notfall- und Krisenplan Chemieunfall

6.3 Brandschutzplan als integraler Bestandteil

Ein Brandschutzplan (ggf. in Kombination mit einem Brandschutzkonzept) gehört in jedem Wäschereibetrieb zur Pflichtdokumentation – nicht nur aus rechtlicher Sicht (z. B. Brandschutzverordnung, Bauordnungen der Länder), sondern auch als elementarer Bestandteil des BCM

Brandschutzkonzept

= Strategische, umfassende Gesamtdarstellung des vorbeugenden Brandschutzes

Zweck:
Ein **Brandschutzkonzept** beschreibt umfassend, wie der bauliche, technische und organisatorische Brandschutz in einem Gebäude oder Betrieb sichergestellt wird – insbesondere bei Sonderbauten, genehmigungspflichtigen Vorhaben und ist heutzutage Bestandteil eines Bauantrags.

Typische Inhalte:

- Gebäude- und Nutzungsklasse (nach Bauordnung)
- Beschreibung des Brandrisikos
- Flucht- und Rettungswegkonzept
- Brand- und Rauchabschnittsbildung
- Löschwasserversorgung
- Anforderungen an Bauteile und Materialien
- Technische Anlagen (z. B. Brandmeldeanlage, Sprinkler)

- Brandschutzmaßnahmen bei besonderen Nutzungen (z. B. Wäschereien, chemische Stoffe)
- Organisation (z. B. Brandschutzordnung, Schulungen)

Erstellt von:
Brandschutzsachverständige, Fachplaner oder Architekten (z. T. bei Sonderbauten gesetzlich gefordert)

Brandschutzplan

= Grafische Darstellung von brandschutzrelevanten Maßnahmen und Einrichtungen

Zweck:
Ein **Brandschutzplan** dient der **Visualisierung** der im Konzept definierten Maßnahmen – z. B. für Rettungskräfte, Aufsichtsbehörden, Bauunternehmen oder das Gebäudemanagement. Er ist **Teil des Brandschutzkonzepts**, aber auch separat einsetzbar.

Typische Inhalte (als Planzeichnung):
- Flucht- und Rettungswege
- Lage von Feuerlöschern, Wandhydranten, Brandmeldern (Flucht - und Rettungsplan)
- Brandabschnitte / Rauchabschnitte
- Nutzungseinheiten und Brandlasten
- Zugangsmöglichkeiten für Feuerwehr (Angriffswege)
- Feuerwehrzufahrten, Aufstellflächen, Löschwasserentnahmestellen

Erstellt von:
Fachplaner oder Architekt auf Grundlage des Brandschutzkonzepts oder der Bauunterlagen

Flucht- und Rettungsplan

= Grafische Darstellung von Brandschutzinhalten für die Mitarbeitenden/ Nutzer/ Besucher

Zweck:
Ein **Flucht- und Rettungsplan** beinhaltet alle Informationen, die Gebäudenutzer benötigen, um im Brandfall richtig agieren zu können (z.B. über Brandschutzordnung Teil A) und auch über die dargestellten Rettungswege eine Orientierung zum Verlassen des Gebäudes erhalten.

Typische Inhalte:
- Flucht- und Rettungswege
- Verhaltensregeln im Brandfall/ Brandschutzordnung Teil A
- Lage von Feuerlöschern, Wandhydranten, Brandmeldern

Erstellt von:
Sachkundige für Flucht- und Rettungspläne, Fachplaner oder Architekten (z. T. bei Sonderbauten gesetzlich gefordert)

Feuerwehrpläne

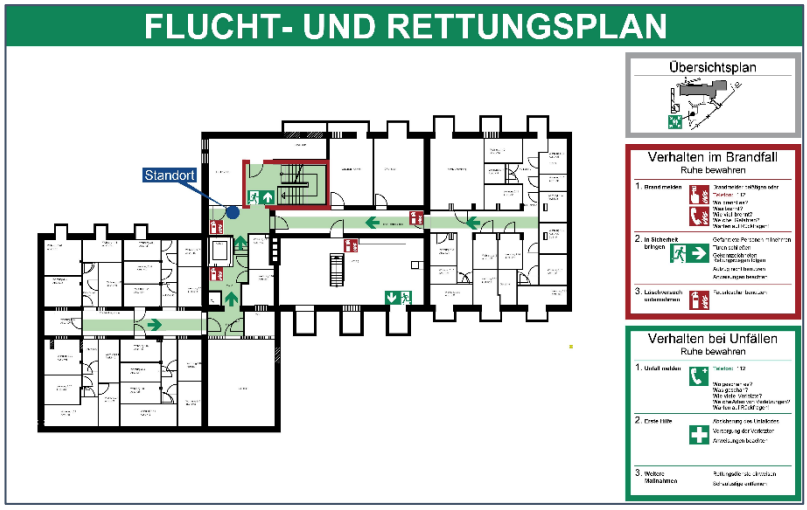
= Grafische Darstellung von Brandschutzinhalten für die Feuerwehr

Zweck:
Ein **Feuerwehrplan** beinhaltet alle Informationen, die die Feuerwehr in die Lage versetzt, wirksame Löscharbeiten vorzunehmen und somit Betriebsschäden zu minimieren.

Typische Inhalte:
- Ansprechpartner
- Löschwasserversorgung
- Brandabschnitte

Erstellt von:
Sachkundige für Feuerwehrpläne, Fachplaner oder Architekten (z. T. bei Sonderbauten gesetzlich gefordert)

Neben dem Brandschutzplan sollte ein IT-Notfallplan Bestandteil des gesamten Notfallmanagements sein. Beide Dokumente ergänzen sich, da sowohl physische Schadensereignisse als auch Cybervorfälle zu erheblichen Betriebsunterbrechungen führen können. Ein integrierter Ansatz verbessert die Reaktionsfähigkeit des Unternehmens.



Quelle: 1https://brandschutz-jaeger.de/images/bilder/FRP_Kellergeschoss_1.jpg

All diese Unterlagen sind regelmäßig auf Aktualität zu prüfen, ggf. mit der örtlichen Feuerwehr abzustimmen und in das Gesamtsystem des Notfallmanagements zu integrieren.

6.4 Kontaktlisten und Ressourcenpläne

Aktuelle Kontaktlisten und Ressourcenpläne sind ein unverzichtbarer Bestandteil jedes BCM-Systems. Sie stellen sicher, dass im Notfall schnell auf relevante Informationen zugegriffen werden kann. Empfohlene Inhalte:

- Ansprechpartner im Krisenteam (mit Mobilnummer, E-Mail)

- Externe Kontakte: Feuerwehr, Polizei, Krankenhaus, Entsorger, Energieversorger, IT-Dienstleister, Techniker
- Lieferanten- und Kundenkontakte
- Übersicht über Ressourcen: Ersatzmaschinen, Notstromaggregate, Chemikalienlager, Reservefahrzeuge
- Plan zur Personalumverteilung bei Engpässen

Diese Informationen sollten sowohl digital (z. B. in Cloud-Backups) als auch analog (z. B. in Krisenordnern vor Ort) vorliegen – mit regelmäßiger Pflege und Aktualisierung.

7 Schulungen, Training & Übungen

Ein Business Continuity Management (BCM) System kann nur dann im Ernstfall wirksam funktionieren, wenn Mitarbeitende auf Krisensituationen vorbereitet sind. Schulungen, regelmäßige Unterweisungen und praxisnahe Übungen sind deshalb unverzichtbare Bestandteile des BCM – insbesondere in systemrelevanten Branchen wie der Wäschereibranche, wo Hygiene, Sicherheit und Versorgungskontinuität oberste Priorität haben.

7.1 Regelmäßige Unterweisungen (inkl. Brandschutzübungen)

Gemäß § 12 Arbeitsschutzgesetz sind Unternehmen verpflichtet, ihre Beschäftigten regelmäßig über Gefährdungen und Verhaltensregeln zu unterweisen – dies gilt auch für BCM-relevante Themen wie Notfallmanagement, Räumungs-/ Evakuierungsabläufe oder Brandverhalten.

Unterweisungsinhalte im Kontext des BCM:

- Verhalten bei Stromausfall, Maschinenstörung oder Chemieunfall
- Evakuierung im Brandfall (inkl. Sammelstellen)
- Kommunikation im Notfall (z. B. an wen wird was gemeldet?)
- Nutzung von Notausgängen, Feuerlöschern und Erste-Hilfe-Einrichtungen
- Rollenverständnis im Krisenstab bzw. Notfallteam
- Betriebsinterne Wiederanlaufverfahren

Frequenz:

- Mindestens einmal jährlich
- Zusätzlich bei Neueinstellungen, Veränderungen im Betrieb oder nach Zwischenfällen

Brandschutzübungen:
Diese können in Abstimmung mit der örtlichen Feuerwehr geplant und dokumentiert werden (siehe ASR A2.2). Sie dienen der Einübung von Fluchtwegen, Alarmierungsketten und Löschmaßnahmen.

Neben Brandschutz- und Notfallübungen sollten Mitarbeitende regelmäßig zu Cyber-Sicherheitsrisiken unterwiesen werden.
Inhalte können sein:

- Phishing erkennen,

- sichere Passwörter,
- Umgang mit mobilen Geräten,
- Meldewege bei IT-Sicherheitsvorfällen,
- Verhalten bei Verdacht auf Schadsoftware,
- Datenschutz und Informationssicherheit.

Die Sensibilisierung der Beschäftigten stellt einen wesentlichen Bestandteil der Cyber-Resilienz dar.

7.2 Simulation von Notfällen

Theoretisches Wissen allein reicht nicht aus – die praktische Simulation realitätsnaher Szenarien ist ein zentraler Bestandteil eines wirksamen BCM. Sie hilft, Schwachstellen zu erkennen, Reaktionssicherheit zu trainieren und die Zusammenarbeit im Team zu stärken.

Beispiele für praxisnahe Notfall-Simulationen in der Wäschereibranche:

- Totalausfall der Energieversorgung mit anschließender Wiederanlaufübung
- Simulation eines Maschinenbrandes mit Evakuierung und Feuerwehranruf
- Ausfall des Hauptlieferanten für Waschmittel – Krisenteam-Simulation zur kurzfristigen Beschaffung
- Pandemie- oder Personalausfallszenario mit Personalumverteilung und Notbesetzung (Lösung: Vertreterregelung)

Empfehlung laut ISO 22301:

- Mindestens einmal pro Jahr eine umfassende Krisensimulation (z. B. Tischübung, Live-Übung, Rollenspiel) oder bei wesentlichen Änderungen im Betrieb, Prozessen oder Personal
- In größeren Betrieben: Übungen für unterschiedliche Hierarchieebenen

7.3 Dokumentation der Übungen

Alle Schulungen, Unterweisungen und Übungen müssen nachvollziehbar dokumentiert werden. Dies dient nicht nur der Nachweispflicht gegenüber Aufsichtsbehörden und Berufsgenossenschaften, sondern auch der kontinuierlichen Verbesserung des BCM-Systems.

Pflichtinhalte der Dokumentation:

- Thema und Ziel der Übung bzw. Unterweisung
- Datum und Uhrzeit
- Beteiligte Personen / Teilnehmerlisten
- Verantwortliche Durchführende (z. B. Brandschutzbeauftragter, QM-Beauftragter)
- Ergebnisse, Beobachtungen, Verbesserungsvorschläge
- ggf. Nachbesserungen am Notfallplan

Aufbewahrungspflicht:
Mindestens 5 Jahre (analog zur DGUV-Empfehlung und internen Auditverfahren nach ISO 22301 / ISO 9001)

8 Überprüfung & Verbesserung

Ein Business Continuity Management (BCM) ist kein statisches System. Seine Wirksamkeit hängt maßgeblich davon ab, wie regelmäßig es geprüft, angepasst und verbessert wird. In einer dynamischen Branche wie der Textilpflege – geprägt durch technologische Entwicklungen, gesetzliche Anforderungen und externe Risiken (z. B. Pandemien, Energiekrisen) – ist die kontinuierliche Weiterentwicklung besonders entscheidend.

Im Rahmen interner Audits sollten auch die Wirksamkeit der IT-Notfallmaßnahmen sowie der Cyber-Resilienz regelmäßig bewertet werden. Hierzu gehören beispielsweise:

- Wiederherstellungstests von Datensicherungen,
- Überprüfung der Backup-Strategie,
- Bewertung von Cyber-Sicherheitsvorfällen,
- Aktualität von Notfallkontakten,
- Durchführung von Penetrationstests oder Schwachstellenanalysen,
- Lessons Learned nach IT-Störungen.

8.1 Regelmäßige Audits

Die Wirksamkeit des BCM-Systems sollte in regelmäßigen internen Audits sowie durch gezielte Tests überprüft werden. Dies ermöglicht eine systematische Beurteilung, ob Prozesse, Notfallpläne, Schulungen und Ressourcen dem tatsächlichen Bedarf entsprechen.
Empfohlene Maßnahmen:

- Interne Audits gemäß ISO 22301 – mindestens jährlich
- Praxistests von Notfallplänen (z. B. Stromausfall, Lieferkettenunterbrechung, Brandszenario)
- Überprüfung technischer Ausrüstungen (Notstrom, Löschsysteme, IT-Backups)
- Audit-Checklisten mit Fokus auf BCM-relevante Prozesse (z. B. OP-Wäsche-Versorgung, Waschmittelversorgung, Fuhrpark)

Die BCM-Prüfung kann effizient in bestehende Auditprozesse (z. B. Qualitäts- oder Hygieneaudits nach RABC oder DTV-Zertifizierung) integriert werden.

Weiterführende Infos/ Tools:
- Formular Audits/ Übungen/ Tests

8.2 Auswertung von Vorfällen und Beinahe Ereignissen

Jeder Vorfall – sei es ein realer Notfall oder ein sogenanntes *Beinahe-Ereignis* – liefert wichtige Erkenntnisse über Schwächen im System und Verbesserungspotenzial.
Typische Vorfälle in der Branche:

- Strom- oder Wasserausfall mit Lieferverzögerung
- Maschinenstillstand durch technische Defekte

- Gefahrstoffleckage in der Dosieranlage
- Brandschäden durch Flusenansammlung oder Hitzeentwicklung
- Personalausfall durch Krankheit oder Unfall

Vorgehen bei der Auswertung:

1. Sofortmeldung und Ereignisprotokoll
2. Analyse der Ursachen (Root Cause Analysis)
3. Bewertung der Auswirkungen auf betroffene Geschäftsprozesse
4. Ableitung von Maßnahmen zur Vermeidung oder Schadensbegrenzung
5. Überarbeitung von Plänen, Abläufen oder Schulungen

Normative Vorgaben

Nach ISO 22301 sind Organisationen verpflichtet, „lessons learned“ systematisch auszuwerten und in das BCM-System einfließen zu lassen. Auch nach dem Arbeitsschutzgesetz (§ 5 ArbSchG) sind Gefährdungsbeurteilungen regelmäßig auf neue Erkenntnisse hin anzupassen.

8.3 Anpassung der Pläne an neue Risiken

Neue Risiken können sich aus gesellschaftlichen, ökologischen oder wirtschaftlichen Entwicklungen ergeben – z. B. durch geopolitische Krisen, Energieknappheit, Digitalisierung, Klimawandel oder Pandemien. Diese Veränderungen müssen **proaktiv** im BCM berücksichtigt werden.

Beispiele für neue Risikofaktoren:

- Extremwetter bspw. Überschwemmungen, Hitzeperioden
- Cyberangriffe auf digitalisierte Steuerungssysteme
- CO_2-Abgaben als Kostenrisiko in der Energieversorgung
- Wassermangel / Wasseraufbereitungspflichten
- Pandemien und deren Auswirkungen auf Personalverfügbarkeit
- Lieferengpässe durch politische Instabilität

Anpassung erfolgt durch:

- Aktualisierung der Risikoanalyse und Business Impact Analysis (BIA)
- Überarbeitung der Notfall- und Krisenpläne
- Einbindung neuer Ressourcen oder Prozesse (z. B. alternative Lieferanten, Digitalisierung von Kommunikation)
- Anpassung der Schulungsinhalte

Empfehlung gemäß ISO 22301:

Das BCM-System sollte mindestens **einmal jährlich** überprüft und bei Bedarf aktualisiert werden – insbesondere nach relevanten Ereignissen oder Änderungen der Rahmenbedingungen.

Weiterführende Infos/ Tools:
Nutzen Sie die TEXSUS-Checkliste „Audit & Verbesserung BCM“ sowie das „Vorfallprotokoll inkl. Ursachenanalyse“. So stellen Sie sicher, dass Ihr BCM nicht nur dokumentiert, sondern auch lebendig, lernfähig und zukunftsorientiert ist.

Weiterführende Infos/ Tools:

- Formular Checkliste Audit & Verbesserung BCM
- Formular Vorfallprotokoll inkl. Ursachenanalyse

8.4 Berücksichtigung von NIS-2 und KRITIS-Anforderungen

Die zunehmende Digitalisierung von Produktions- und Geschäftsprozessen führt dazu, dass neben klassischen Gefahren wie Brand, Energieausfall oder Lieferengpässen auch Cyberrisiken zu den wesentlichen Bedrohungen für die Geschäftskontinuität gehören. Business Continuity Management (BCM) und Informationssicherheit sind daher eng miteinander verknüpft und sollten als integrale Bestandteile eines ganzheitlichen Risikomanagements betrachtet werden.

Mit der europäischen NIS-2-Richtlinie sowie deren Umsetzung in nationales Recht werden die Anforderungen an die Cybersicherheit und Resilienz zahlreicher Unternehmen deutlich erweitert. Ziel ist es, die Widerstandsfähigkeit kritischer und wichtiger Einrichtungen gegenüber Cyberangriffen und anderen Sicherheitsvorfällen nachhaltig zu stärken.

Für Unternehmen der Wäscherei- und Textilreinigungsbranche kann dies insbesondere dann von Bedeutung sein, wenn sie Einrichtungen der Kritischen Infrastruktur (KRITIS) versorgen oder selbst als Teil einer kritischen Lieferkette eingestuft werden. Dies betrifft beispielsweise Unternehmen, die Krankenhäuser, Pflegeeinrichtungen oder andere systemrelevante Einrichtungen regelmäßig mit hygienisch aufbereiteter Wäsche versorgen. Auch wenn ein Betrieb nicht unmittelbar unter die gesetzlichen Anforderungen von NIS-2 oder dem KRITIS-Dachgesetz fällt, erwarten Kunden, Behörden und Versicherungen zunehmend ein angemessenes Sicherheits- und Resilienzniveau.

Ein wirksames Business Continuity Management unterstützt Unternehmen dabei, die organisatorischen Voraussetzungen für diese Anforderungen zu schaffen. Hierzu gehören insbesondere:

- die regelmäßige Bewertung von Cyberrisiken im Rahmen der Risikoanalyse,
- die Identifikation kritischer Informations- und Kommunikationstechnologien,
- die Erstellung und Pflege von IT-Notfall- und Wiederanlaufplänen,
- die Sicherstellung einer funktionierenden Datensicherung und Wiederherstellung,
- die Definition von Melde- und Eskalationswegen bei IT-Sicherheitsvorfällen,
- die Berücksichtigung von Risiken innerhalb der Lieferkette,
- die regelmäßige Sensibilisierung und Schulung der Mitarbeitenden,
- die Durchführung von Übungen und Tests für Cyber- und IT-Notfallszenarien.

Besondere Bedeutung kommt dabei der Zusammenarbeit zwischen Geschäftsleitung, IT-Verantwortlichen, Informationssicherheitsbeauftragten, BCM-Verantwortlichen und externen Dienstleistern zu. Nur ein abgestimmtes Vorgehen ermöglicht es, sowohl physische Schadensereignisse als auch Cybervorfälle wirksam zu beherrschen und die Versorgung kritischer Kunden auch in Krisensituationen aufrechtzuerhalten.

Unternehmen sollten ihre BCM- und Notfallprozesse daher regelmäßig daraufhin überprüfen, ob sie den aktuellen gesetzlichen, normativen und vertraglichen Anforderungen entsprechen. Hierzu zählen insbesondere die Anforderungen der ISO 22301 (Business Continuity Management), der ISO/IEC 27001 (Informationssicherheitsmanagement), der NIS-2-Richtlinie sowie – soweit anwendbar – die Vorgaben des KRITIS-Dachgesetzes und weiterer nationaler Regelungen zur Resilienz Kritischer Infrastrukturen.

Die kontinuierliche Weiterentwicklung der organisatorischen und technischen Sicherheitsmaßnahmen trägt wesentlich dazu bei, Betriebsunterbrechungen zu vermeiden, die Versorgungssicherheit zu gewährleisten und das Vertrauen von Kunden, Behörden und weiteren Stakeholdern nachhaltig zu stärken.

Anhänge (Formulare, Checklisten, Vorlagen)

Formular Checkliste Brandschutzprüfung

Zweck: Die Checkliste dient der regelmäßigen Überprüfung des baulichen, technischen und organisatorischen Brandschutzes sowie der Dokumentation festgestellter Mängel und eingeleiteter Maßnahmen

Allgemeine Angaben

Feld	Eintrag
Unternehmen/Standort	
Geprüfter Bereich	
Datum	
Prüfer	
Nächste Prüfung	

1. Baulicher Brandschutz

Prüffrage	Ja/Nein	Bemerkung/Maßnahme
Brandabschnitte sind unverändert vorhanden?	☐ Ja ☐ nein	
Brandschutztüren schließen selbstständig?	☐ Ja ☐ nein	
Brandschutztüren werden nicht blockiert oder aufgekeilt?	☐ Ja ☐ nein	
Flucht- und Rettungswege sind frei zugänglich?	☐ Ja ☐ nein	
Notausgänge lassen sich jederzeit öffnen?	☐ Ja ☐ nein	
Fluchtwegekennzeichnungen sind vorhanden und gut sichtbar?	☐ Ja ☐ nein	

2. Technischer Brandschutz

Prüffrage	Ja/Nein	Bemerkung/Maßnahme
Brandmeldeanlage betriebsbereit?	☐ Ja ☐ nein	
Löschanlagen funktionsfähig?	☐ Ja ☐ nein	
Feuerlöscher vollständig vorhanden?	☐ Ja ☐ nein	
Feuerlöscher geprüft (DIN 14406)?	☐ Ja ☐ nein	
Wandhydrant zugänglich?	☐ Ja ☐ nein	
Rauch und Wärmeabzugsanlagen funktionsfähig?	☐ Ja ☐ nein	
Sicherheitsbeleuchtung funktionsfähig?	☐ Ja ☐ nein	
Notstromversorgung geprüft?	☐ Ja ☐ nein	

3. Organisatorischer Brandschutz

Prüffrage	Ja/Nein	Bemerkung/Maßnahme
Brandschutzordnung aktuell?	☐ Ja ☐ nein	
Brandschutzordnung Teil A ausgehängt?	☐ Ja ☐ nein	
Brandschutzhelfer ausreichend vorhanden?	☐ Ja ☐ nein	
Mitarbeitende jährlich unterwiesen?	☐ Ja ☐ nein	
Fremdfirmen eingewiesen?	☐ Ja ☐ nein	
Alarmierungskette aktuell?	☐ Ja ☐ nein	
Feuerwehrpläne aktuell?	☐ Ja ☐ nein	

4. Produktions- und Lagerbereiche

Prüffrage	Ja/Nein	Bemerkung/Maßnahme
Flusen regelmäßig entfernt?	☐ Ja ☐ nein	
Maschinen sauber und gewartet?	☐ Ja ☐ nein	
Chemikalien ordnungsgemäß gelagert?	☐ Ja ☐ nein	
Sicherheitsdatenblätter vorhanden?	☐ Ja ☐ nein	
Heiße Wäsche wird nicht unkontrolliert gelagert?	☐ Ja ☐ nein	
Elektrische Anlagen ohne erkennbare Mängel?	☐ Ja ☐ nein	

5. Dokumentation

Prüffrage	Ja/Nein	Bemerkung/Maßnahme
Wartungsnachweise vorhanden?	☐ Ja ☐ nein	
Prüfprotokolle vollständig?	☐ Ja ☐ nein	
Mängel dokumentiert?	☐ Ja ☐ nein	
Maßnahmen terminiert‘?	☐ Ja ☐ nein	

Festgelegte Mängel

Nr.	Beschreibung	Priorität	Verantwortlich	Termin
		☐ Hoch ☐ Mittel ☐ Niedrig		

Gesamtbewertung

☐	Keine Mängel
☐	Geringe Mängel
☐	Wesentliche Mängel
☐	Kritische Mängel – Sofortmaßnahmen erforderlich

Unterschrift Prüfer:	
Unterschrift Verantwortliche/r:	

Formular Checkliste Evakuierungsplan

Zweck: Die Checkliste dient der Überprüfung der organisatorischen und technischen Voraussetzungen für eine sichere und wirksame Evakuierung im Notfall.

Allgemeine Angaben

Feld	Eintrag
Unternehmen/Standort	
Bereich	
Datum	
Prüfer	

1. Evakuierungsplan

Prüffrage	Ja/Nein	Bemerkung/
Aktueller Evakuierungsplan vorhanden?	☐ Ja ☐ nein	
Flucht- und Rettungspläne aktuell?	☐ Ja ☐ nein	
Sammelstelle definiert?	☐ Ja ☐ nein	
Alternativwege festgelegt	☐ Ja ☐ nein	
Alarmierungswege dokumentiert?	☐ Ja ☐ nein	

2. Flucht- und Rettungswege

Prüffrage	Ja/Nein	Bemerkung/
Fluchtwege frei?	☐ Ja ☐ nein	
Türen nicht verschlossen?	☐ Ja ☐ nein	
Notausgänge gekennzeichnet?	☐ Ja ☐ nein	
Sicherheitsbeleuchtung funktionsfähig?	☐ Ja ☐ nein	
Rettungspläne gut sichtbar?	☐ Ja ☐ nein	

3. Organisation

Prüffrage	Ja/Nein	Bemerkung/
Evakuierungshelfer benannt?	☐ Ja ☐ nein	
Brandschutzhelfer ausreichend vorhanden?	☐ Ja ☐ nein	
Aufgaben dokumentiert?	☐ Ja ☐ nein	
Vertretungsregelungen vorhanden?	☐ Ja ☐ nein	

4. Alarmierung

Prüffrage	Ja/Nein	Bemerkung/
Alarmierung funktioniert?	☐ Ja ☐ nein	
Lautsprecheranlage funktionsfähig?	☐ Ja ☐ nein	
Alternativ Alarmierung vorhanden?	☐ Ja ☐ nein	
Alarmierungskette aktuell	☐ Ja ☐ nein	

5. Übung

Prüffrage	Ja/Nein	Bemerkung/
Evakuierungsübung innerhalb der letzten 12 Monate durchgeführt?	☐ Ja ☐ nein	
Übung dokumentiert?	☐ Ja ☐ nein	
Verbesserungsmaßnahmen umgesetzt?	☐ Ja ☐ nein	
Mitarbeitende unterwiesen?	☐ Ja ☐ nein	

6. Besondere Personengruppen

Prüffrage	Ja/Nein	Bemerkung/
Besucher berücksichtigt?	☐ Ja ☐ nein	
Fremdfirmen berücksichtigt?	☐ Ja ☐ nein	
Personen mit eingeschränkter Mobilität berücksichtigt?	☐ Ja ☐ nein	
Sammelplatzkontrolle geregelt?	☐ Ja ☐ nein	

7. Nach der Evakuierung

Prüffrage	Ja/Nein	Bemerkung/
Vollzähligkeitskontrolle geregelt?	☐ Ja ☐ nein	
Kommunikation mit Feuerwehr geregelt?	☐ Ja ☐ nein	
Rückkehr in das Gebäude geregelt?	☐ Ja ☐ nein	
Ereignis dokumentiert?	☐ Ja ☐ nein	

Festgestellte Mängel

Nr.	Beschreibung	Priorität	Verantwortlich	Termin
		☐ Hoch ☐ Mittel ☐ Niedrig		

Gesamtbewertung

☐	Keine Mängel
☐	Geringe Mängel
☐	Wesentliche Mängel
☐	Sofortmaßnahmen erforderlich

Unterschrift Prüfer:	
Unterschrift Verantwortliche/r:	

Formular Alarmierungs- und Notfallplan

Zweck: Dieses Formular dient der strukturierten Dokumentation der internen und externen Alarmierungs- und Eskalationskette im Krisen- oder Störungsfall (z. B. Stromausfall, Brand, IT-Ausfall, Wasserschaden, Chemikalienleck).

Allgemeine Angaben

Feld	Eintrag
Unternehmen / Standort	
Version der Alarmierungskette	
Gültig ab / Letzte Aktualisierung	
Erstellt von	

Sofortmaßnahmen:

Alarmieren

- → Ruhe bewahren
- → Brandmelder betätigen (falls vorhanden)

- → ☎ Feuerwehr: **112**
- → ☎ Polizei: **110**
- → ☎ Rettungsdienst: **112**

Notruf absetzen (5-W-Regel)

Fragen beantworten
Wer meldet?
Wo ist das Ereignis?
Was ist passiert?
Wie viele Personen sind betroffen/verletzt?
Warten auf Rückfragen

Personen schützen

☐ Personen im Gefahrenbereich warnen
☐ Hilfsbedürftige Personen unterstützen
☐ Aufzüge nicht benutzen
☐ Fluchtwege nutzen
☐ Türen schließen (nicht abschließen)
☐ Sammelplatz aufsuchen

Übersicht – Alarmierungsstufen

Stufe	Ereignisart / Auslöser	Zuständigkeit	Maßnahmen
Stufe 1	z. B. Störung in Teilbereich, kein Produktionsstopp	Bereichsleitung	Interne Information, Erstmaßnahmen
Stufe 2	z. B. Produktionsstillstand, IT-Ausfall, Personalausfall	Geschäftsleitung / BCM-Verantwortliche	Aktivierung Notfallteam, ggf. externe Stellen
Stufe 3	z. B. Brand, Gefahrstoffaustritt, externe Bedrohung	Geschäftsleitung, Behörden	Alarmierung Feuerwehr, Polizei, Evakuierung

Alarmierungskette intern

Position / Funktion	Name	Telefon dienstlich / mobil	E-Mail	Vertretung
Geschäftsleitung				
Brandschutzhelfer				
Evakuierungshelfer				
Ersthelfer				
Produktionsleitung				
Haustechnik / Energie				
IT-Verantwortliche/r				
Personalverantwortung				
Sicherheitsbeauftragte/r				

Alarmierungskette extern

Organisation / Partner	Kontaktperson	Erreichbarkeit	Notfallnummer	Bemerkung
Feuerwehr (112)		rund um die Uhr	112	automatisch alarmieren
Polizei (110)		rund um die Uhr	110	bei Bedrohung, Einbruch
Energieversorger				z. B. Stromausfall
IT-Dienstleister				z. B. Serverausfall

Gebäudeverwaltung / Wartung				z. B. Wasserrohr-bruch
Leasing-/Fuhrpark-dienstleister				bei Fahrzeugaus-fall
Versicherer				Schadenmel-dung
Weitere:				

Kommunikationsmittel

☐ Telefonkette aktiviert	☐ Notfallliste aushängend	☐ Alarm-SMS-System
☐ Lautsprecher / Durchsage	☐ E-Mail-Verteiler	☐ Messenger-Gruppe (z. B. Signal)

Abschluss des Ereignisses

☐ Vollzähligkeit geprüft

☐ Fehlende Personen gemeldet

☐ Feuerwehr eingewiesen

☐ Schaden dokumentiert

☐ Geschäftsleitung informiert

☐ Wiederanlaufmaßnahmen eingeleitet

☐ Ereignis abgeschlossen

Dokumentation der Alarmierung (im Ereignisfall ausfüllen)

Datum / Uhr-zeit	Wer hat infor-miert?	Wen wurde infor-miert?	Maßnahme / Reak-tion	Unterschrift

Formular Notfall und Krisenplan – Chemieunfall

Standort/Betrieb	
Version	
Gültig ab /	
Erstellt von	
Geprüft am	

Notfallbeschreibung / Szenario

Aspekt	**Beschreibung**
Möglicher Vorfall:	☐ Leckage ☐ Überlauf ☐ Verwechslung ☐ Dampfentwicklung ☐ Reaktion / Explosion ☐ Sonstiges: _____
Beteiligte Stoffe:	_____ (z. B. Chlor, Natronlauge, Säuren etc.)
Ort des Vorfalls:	_____ (z. B. Lager, Dosieranlage, Waschstraße)
Betroffene Bereiche / Personen:	

Sofortmaßnahmen

Maßnahme	**Verantwortlich**	**Zeit / Status**
Alarmierung interner Notfallkontakte (siehe Abschnitt 5)		_____ Uhr ☐ erledigt
Evakuierung gefährdeter Personen		_____ Uhr ☐ erledigt
Absperrung und Kennzeichnung des Bereichs		_____ Uhr ☐ erledigt
Erste Hilfe / Versorgung von Verletzten		_____ Uhr ☐ erledigt
Nutzung PSA (Persönliche Schutzausrüstung)		_____ Uhr ☐ erledigt
Unterbrechen der Zufuhr / Energie / Wasser		_____ Uhr ☐ erledigt

Lüftung / Belüftung einschalten (sofern sicher)		_____ Uhr ☐ erledigt

Externe Stellen alarmieren

Organisation	Telefonnummer	Benachrichtigt um	Ansprechpartner
Feuerwehr (112)	112	_____ Uhr ☐	
Giftnotruf		_____ Uhr ☐	
Polizei		_____ Uhr ☐	
Umweltbehörde		_____ Uhr ☐	
Entsorgungsunternehmen		_____ Uhr ☐	
Fachberater (Chemikalienliefe-rant)		_____ Uhr ☐	

Folgemaßnahmen & Dokumentation

Maßnahme	Verantwortlich	Erledigt
Eintrag ins Verbandbuch / Unfallbericht		☐ Ja
Interne Meldung an Geschäftsleitung / BCM		☐ Ja
Protokoll der betroffenen Stoffe / Mengen		☐ Ja
Entsorgung / Dekontamination beauftragt		☐ Ja
Wiederherstellung sicherer Betriebszustände		☐ Ja
Ursachenanalyse begonnen		☐ Ja
Behördenbericht / Anzeige erstattet (falls erforderlich)		☐ Ja

Interne Notfallkontakte

Funktion	Name	Telefon	Mobil
Geschäftsführung			
Notfallbeauftragte*r / BCM			
Sicherheitsbeauftragte*r			
Lager / Technikleitung			
Ersthelfer*in vor Ort			

Kommunikationsmaßnahmen

Zielgruppe	Maßnahme	Zeitpunkt	Verantwortlich
Mitarbeitende vor Ort	Sicherheitsunterweisung / Aushang	_____ Uhr	
Kunden / Partner	Info bei Lieferverzögerung etc.	_____ Uhr	
Öffentlichkeit / Presse	Nur nach Freigabe durch GF / Behörden	_____ Uhr	

Lessons Learnd / Nachbereitung (innerhalb 72 h)

Punkt	Verantwortlich	Status / Termin
Team-Nachbesprechung durchgeführt		☐ erledigt am: _____
Schwachstellenanalyse / Verbesserungsmaßnahmen geplant		☐ geplant bis: _____
Checklisten / Notfallpläne aktualisiert		☐ geplant bis: _____
Schulungsbedarf identifiziert		☐ Ja / ☐ Nein

Unterschrift Einsatzleitung / Dokumentierende Persom	
Datum	

Formular Audits / Übung / Tests

Audit- und Testplan für das BCM-System

Ziel: Sicherstellen, dass das Business Continuity Management-System (BCMS) wirksam, aktuell und im Ernstfall funktionsfähig ist.

Empfehlung: Kombination aus organisatorischen Audits und praktischen Tests / Übungen auf allen Ebenen – jährlich oder risikobasiert.

1. Interne BCM-Audits

Auditart	Zielsetzung	Häufigkeit	Verantwortlich	Dokumentation
Systemaudit BCM	Bewertung der Gesamtstruktur, Rollen, Verfahren, Aktualität	jährlich	BCM-Beauftragte*r / QMB	Auditbericht mit Maßnahmenliste
Prozessaudit (kritische Prozesse)	Prüfung der Notfallpläne und Wiederanlaufstrategien je Prozess	alle 2 Jahre oder bei Änderungen	Bereichsleitung + BCM	Prüfprotokoll je Bereich
Dokumentenprüfung	Aktualität der Pläne, Alarmierungslisten, Kontaktdaten	halbjährlich	BCM-Verantwortung	Änderungsnachweis
Lieferkettenprüfung (BC-Risiken)	Bewertung der Resilienz kritischer Lieferanten / Logistikpartner	jährlich	Einkauf / BCM / ggf. Compliance	Lieferanten-Scorecard, Risikoübersicht

2. Notfalltests und Übung

Testart	Beschreibung	Zielsetzung	Häufigkeit	Beteiligte
Alarmierungsübung (stille oder offene Übung)	Test der Erreichbarkeit und Reaktionszeit gemäß Alarmierungskette	Funktionsfähigkeit der Kommunikation	1–2 × jährlich	Notfallteam, Schlüsselpersonen
Evakuierungsübung	Probeweise Räumung eines Gebäudeteils	Reaktion auf Gefahrenlage, Schulung der Mitarbeitenden	jährlich	Alle Mitarbeitenden
Tabletop-Übung (Planspiel)	Szenariobasierte Durchspielung eines Vorfalls im Meetingformat	Entscheidungswege, Koordination, Schwachstellenanalyse	jährlich oder bei Änderung	Geschäftsleitung, Führungskräfte
IT-Notfalltest	Test von Datenwiederherstellung, Backup, Umschaltprozessen	Verfügbarkeit kritischer IT-Systeme	jährlich oder halbjährlich	IT / Externe IT-Dienstleister
Versorgungsausfall-Übung	Simulation von Strom-, Wasser- oder Wärmeausfall	Prüfung Notfallpläne, Ersatzversorgung (z. B. Notstrom)	alle 2–3 Jahre	Technik / Energie / Produktion
Kooperationsübung mit Partnerbetrieben	Test der Ersatzversorgung (z. B. durch Partnerwäscherei)	Praktikabilität von Ausweichstrategien	alle 3–4 Jahre	Partnerunternehmen, Logistik

3. Auswertung und Verbesserungen

Element	Maßnahmen
Nachbereitung jeder Übung	Kurzes Protokoll, Bewertung (Was lief gut? Wo klemmt's?), Lessons Learned
Maßnahmenplan (BCM-Verbesserung)	Sammlung aller offenen Punkte aus Audits/Tests mit Fristen und Verantwortlichen
BCM-Managementreview	Einmal jährlich – Auswertung aller Ergebnisse, Fortschritte, Änderungsbedarf
Bericht an Geschäftsleitung	Status BCM, Risiken, offene Punkte – idealerweise als Bestandteil des Nachhaltigkeits- oder Risikoberichts

Formular Audit & Verbesserung BCM

Zweck: Zur systematischen Durchführung und Dokumentation eines internen BCM-Audits gemäß dem TEXSUS-Leitfaden. Die Checkliste unterstützt Wäscherei- und Reinigungsbetriebe bei der kontinuierlichen Verbesserung ihrer Notfall- und Wiederanlaufstrukturen.

Allgemeine Angaben

Element	Eintrag
Auditdatum	
Standort / Bereich	
Auditor*in	
BCM-Verantwortliche*r	
Version des BCM-Plans	

Systemprüfung

Prüffrage	Erfüllt? (Ja/Nein/Teilw.)	Bemerkung / Maßnahme
Ist ein aktueller BCM-Plan vorhanden?	☐ Ja ☐ Nein ☐ Teilw.	
Ist der BCM-Plan versioniert und freigegeben?	☐ Ja ☐ Nein ☐ Teilw.	
Sind Verantwortlichkeiten im Notfall klar definiert?	☐ Ja ☐ Nein ☐ Teilw.	
Gibt es dokumentierte Notfall- und Wiederanlaufpläne?	☐ Ja ☐ Nein ☐ Teilw..	
Wurden innerhalb der letzten 12 Monate Tests oder Übungen durchgeführt?	☐ Ja ☐ Nein ☐ Teilw..	
Wurde die Alarmierungskette zuletzt überprüft / getestet?	☐ Ja ☐ Nein ☐ Teilw.	
Sind alle kritischen Prozesse priorisiert dokumentiert?	☐ Ja ☐ Nein ☐ Teilw.	
Gibt es Schulungsnachweise für BCM-relevante Personen?	☐ Ja ☐ Nein ☐ Teilw..	
Wurden externe Partner / Lieferanten in BCM einbezogen?	☐ Ja ☐ Nein ☐ Teilw.	
Wurde ein BCM-Review durch die Geschäftsleitung durchgeführt?	☐ Ja ☐ Nein ☐ Teilw.	

Verbesserung und Lessons Learned

Prüffrage	Bewertung	Geplante Maßnahme / Verantwortlich / Frist
Wurden aus Vorfällen oder Tests konkrete Verbesserungen abgeleitet?	☐ Ja ☐ Nein	
Ist ein Maßnahmenplan mit Fristen dokumentiert?	☐ Ja ☐ Nein	
Gibt es dokumentierte „Lessons Learned"-Protokolle?	☐ Ja ☐ Nein	
Wird der BCM-Plan regelmäßig aktualisiert (mind. jährlich)?	☐ Ja ☐ Nein	
Bestehen erkennbare organisatorische oder technische Schwachstellen?	☐ Ja ☐ Nein	

Auditbewertung (Gesamteindruck)

Kriterium	Bewertung
BCM-Struktur	☐ sehr gut ☐ gut ☐ verbesserungswürdig
Notfallvorbereitung	☐ sehr gut ☐ gut ☐ verbesserungswürdig
Umsetzung in der Praxis	☐ sehr gut ☐ gut ☐ verbesserungswürdig
Kommunikationswege	☐ sehr gut ☐ gut ☐ verbesserungswürdig

📝 Fazit / Handlungsempfehlungen:

Unterschrift Auditor* in		**Datum**	
Unterschrift BCM-Verantwortliche*r		**Datum**	

Formular Vorfallprotokoll inkl. Ursachenanalyse

Zweck: Dokumentation und Nachverfolgung von Notfällen, Beinahe-Ereignissen oder Störungen. Die Analyse dient der Ursachenklärung und Ableitung geeigneter Maßnahmen zur BCM-Verbesserung

1. Grunddaten zum Vorfall

Feld	Eintrag
Vorfallsdatum	
Uhrzeit	
Ort / Bereich	
Meldende Person	
Art des Vorfalls	☐ Technisch ☐ Organisatorisch ☐ Extern ☐ IT ☐ Sonstiges:
Kurzbeschreibung	

2. Erstmaßnahmen

Maßnahme	Ausgeführt von	Zeitpunkt	Wirkung
			☐ erfolgreich ☐ begrenzt ☐ keine Wirkung
			☐ erfolgreich ☐ begrenzt ☐ keine Wirkung

3. Auswirkung des Vorfalls

Kategorie	Bewertung / Beschreibung
Betroffene Prozesse	
Dauer der Störung / Ausfallzeit	
Betriebliche Folgen (z. B. Stillstand, Kundeninfo)	
Externe Auswirkungen (Kunden, Partner, Behörden)	
Gefährdung von Personen / Umwelt?	☐ Ja ☐ Nein – Wenn ja:

4. Ursachenanalyse (Root Cause Analysis)

Methode	Beschreibung / Ergebnis
☐ 5-Why-Methode	
☐ Fehlerbaum	
☐ Ishikawa-Diagramm	
Direkte Ursache(n)	
Indirekte / organisatorische Ursache(n)	
Wiederholungsrisiko	☐☐ hoch ☐ mittel ☐ gering

5. Maßnahmen / Lessons Learnd

Maßnahme	Verantwortlich	Termin	Status
			☐ offen ☐ erledigt
			☐ offen ☐ erledigt
Aufnahme in BCM-Plan notwendig?	☐ Ja ☐ Nein	Änderungsvermerk:	

6. Nachverfolgung

Feld	Eintrag
Verantwortlich für Kontrolle	
Kontrolle erfolgt am	
Rückmeldung an BCM-Verantwortliche	☐ Ja ☐ Nein
Folgeaudit / Review geplant?	☐ Ja ☐ Nein, Begründung:

Unterschrift dokumentierende Person		Datum	

Unterschrift BCM-Verantwortliche*r		**Datum**	

Formular Kommunikationsplan im Krisenfall

Ziel: Sicherstellen einer transparenten, schnellen und zielgerichteten Kommunikation bei Betriebsstörungen, um Schäden zu begrenzen, Vertrauen zu erhalten und handlungsfähig zu bleiben.

1. Allgemeine Angaben

Element	Eintrag
Betrieb / Standort	
Verantwortlich für Krisenkommunikation	
Vertretung / Backup	
Version	
Letzte Aktualisierung	

2. Kommunikationsziele

- Sachliche und schnelle **Information der relevanten Zielgruppen**
- Vermeidung von Spekulationen, Gerüchten oder Unsicherheit
- Aufrechterhaltung der **Kundenbindung und öffentlichen Reputation**
- Nachweisbare und dokumentierte Kommunikation (z. B. für Behörden, Versicherungen)

3. Zielgruppen & Kommunikationswege

Zielgruppe	Ziel / Inhalt	Kanal	Frequenz	Ansprechpartner
Kritische Kunden (z. B. Kliniken, Pflegeeinrichtungen)	Sofortige Information über Störung, Verfügbarkeit, Alternativen	Telefon, E-Mail, ggf. Besuch	Sofort, dann mind. täglich	Key Account / Geschäftsleitung
Behörden / Aufsichtsstellen (z. B. Gesundheitsamt, KRITIS-Behörde)	Meldung gem. gesetzlicher Pflicht, Beschreibung Maßnahmen	Telefon + schriftlich	Sofort bei Relevanz	Geschäftsführung
Lieferanten / Logistikpartner	Anpassung Lieferzeiten / Routen / Prioritäten	Telefon, Mail	Bei Bedarf	Einkauf / Logistikleitung
Mitarbeitende	Information über Lage, Aufgaben, Verhalten	Aushang, Mitarbeiter-App, Meetings	Regelmäßig (z. B. 2× täglich)	Bereichsleitungen / HR

Öffentlichkeit / Presse *(nur bei größerer Relevanz)*	Sachliche Information zur Lage, keine Spekulation	Nur über Geschäftsführung oder PR	Situativ	Geschäftsleitung / Externe Kommunikation
Versicherer	Sachverhaltsschilderung, Fristen, Dokumentation	E-Mail + Telefon	Innerhalb 48 h	Controlling / GF

4. Rollen & Zuständigkeiten

Funktion	Verantwortlich für	Name	Kontakt
Geschäftsführung	Freigabe von Kommunikation, Behördenkontakt		
BCM-Beauftragte*r	Koordination, Dokumentation		
Kundenbetreuung	Information kritischer Kunden		
HR / Personal	Interne Kommunikation an Mitarbeitende		
IT / Technik	Kommunikation über technische Wiederherstellung		
Einkauf / Logistik	Abstimmung mit Lieferanten & Transporteuren		

5. Kommunikationsmittel & Vorbereitung

Mittel / Vorlage	Vorhanden?	Bemerkung
Kontaktlisten aller Zielgruppen	☐ Ja ☐ Nein	regelmäßig prüfen
E-Mail-Verteiler / Rufnummernlisten	☐ Ja ☐ Nein	DSGVO-konform verwalten
Textbausteine für Erstinformationen	☐ Ja ☐ Nein	z. B. Versorgungsengpass, IT-Störung
Vorbereitete Infoaushänge für Mitarbeitende	☐ Ja ☐ Nein	z. B. Verhalten im Störfall
Kommunikationsplattform (z. B. Teams, WhatsApp Notfallgruppe)	☐ Ja ☐ Nein	klar definierte Nutzung
Presse-/Behördenstatement (Muster)	☐ Ja ☐ Nein	nur durch Freigabe der GF

6. Ablaufschema im Ernstfall

A	Krisenereignis erkannt
B	Beurteilung durch BCM-Team
B → C	Freigabe durch Geschäftsleitung
C → D1	Kritische Kunden informieren
C → D2	Behörden kontaktieren
C → D3	Lieferanten abstimmen
C → D4	Mitarbeitende informieren
C → D5	Öffentlichkeit ggf. informieren
D1 → E	Laufende Updates & Lösungen kommunizieren
D4 → E	

7. Dokumentation & Nachbereitung

Element	Status	Kommentar
Kommunikationsverlauf protokolliert	☐ Ja ☐ Nein	Datum, Empfänger, Inhalt
Feedback von Kunden / Behörden erfasst	☐ Ja ☐ Nein	zur Nachbereitung
Lessons Learned dokumentiert	☐ Ja ☐ Nein	in BCM-Review übernehmen
Verbesserungsmaßnahmen geplant	☐ Ja ☐ Nein	z. B. Tool, Schulung, Plan aktualisieren

Vorlage Vertretungsregelung bei Personalausfall

Funktion / Stelle	Hauptverantwortlicher	1. Vertretung	2. Vertretung	Kritische Aufgaben	Dokumentation / Ablage
Geschäftsführer	XY	Betriebsleiter	Prokurist	Kundenkommunikation, Krisenentscheidungen, Behördenkontakte	xx
Betriebsleiter	XY	Produktionsleiter	Schichtleiter	Produktionssteuerung, Personalplanung, Wiederanlauf	Arbeitsanweisung Betriebsleitung
Produktionsleiter	XY	Schichtleiter Früh	Schichtleiter Spät	Produktionsplanung, Maschinenbelegung	Produktionshandbuch
Schichtleiter	XY	Vorarbeiter	Produktionsleiter	Personalsteuerung, Störungsmanagement	Schichtführerhandbuch
Technik/Instandhaltung	XY	Stellv. Techniker	Betriebsleiter	Störungsbeseitigung, Versorgungsanlagen	Wartungshandbuch
Dampf-/Kesselanlagenverantwortlicher	XY	Techniker	Externer Dienstleister	Dampferzeugung, Kesselbetrieb	Kesselbuch
Qualitätsmanagement / Hygiene	XY	Laborleitung	Betriebsleiter	RABC, Freigaben, Reklamationen	xx
Disposition / Tourenplanung	XY	Innendienst	Betriebsleiter	Tourenplanung, Kundenaufträge	ERP-System / Prozessbeschreibung
Fuhrparkverantwortlicher	XY	Disponent	Betriebsleiter	Fahrzeugplanung, Fahrereinsatz	Fuhrparkmanagement
IT-Verantwortlicher	XY	Kaufmännische Leitung	Geschäftsführer	ERP, Server, Datensicherung	IT-Notfallplan
Einkauf / Beschaffung	XY	Kaufmännische Leitung	Betriebsleiter	Waschmittel, Textilien, Ersatzteile	Einkaufsprozess
Personalwesen	XY	Kaufmännische Leitung	Geschäftsführer	Lohnabrechnung, Personaleinsatz	xx