Business   
Continuity Plan

Dokumentverlauf

**VERLAUF DER ÄNDERUNGEN**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Geändert von** | Beschreibung der Änderungen (V+1) |
| **xxx** | **xxx** | **xxx** | **xxx** |
| **…** |  |  |  |

**VERLAUF DER GENEHMIGUNGEN**

|  |  |  |
| --- | --- | --- |
| **Name** | **Funktion** | **Datum der Genehmigung durch die höchste Führungsebene (Geschäftsleitung)** |
| **xxx** | **xxx** | **xxx** |
| **…** |  |  |

Dieses Dokument ist gültig ab **[Datum]**.

Dieses Dokument wird wie folgt bewahrt:

1. In Papierform an folgenden Orten: **[Liste der Orte]**.
2. In digitaler Form an folgenden Orten: **[Ort z. B. im Intranet]**.

Eigner dieses Dokuments ist **[Funktion]**. Er prüft mindestens einmal im Jahr, ob Aktualisierungen notwendig sind.

**Inhaltsverzeichnis**

[**Kapitel I Zweck des Dokuments** 4](#_Toc57021120)

[**Kapitel II Verbindungen zwischen den Verfahren** 5](#_Toc57021121)

[**Kapitel III Wählen Sie jemanden an der Spitze** 7](#_Toc57021122)

[3.1 Bestimmen Sie einen Administrator für den Business Continuity Plan 7](#_Toc57021123)

[3.2 Rollen des Administrators des Business Continuity Plan 7](#_Toc57021124)

[**Kapitel IV BUSINESS CONTINUITY PLAN - GESCHÄFTSKONTINUITÄTSKONTINUITÄTSPLAN** 9](#_Toc57021125)

[4.1 Schritt 1: Definition des Umfangs des Business Continuity Plan: 9](#_Toc57021126)

[4.2 Schritt 2: Aktivierung des Plans 10](#_Toc57021127)

[4.3 Schritt 3: Führen Sie die zu ergreifenden Maßnahmen auf 13](#_Toc57021128)

[4.4 Schritt 4: Deaktivierung des Business Continuity Plan 17](#_Toc57021129)

[4.5 Schritt 5: Testen Sie Ihren Plan und halten Sie ihn auf dem Laufenden 18](#_Toc57021130)

[**Kapitel V Anlagen** 19](#_Toc57021131)

[5.1 Anlage 1: Kontaktliste 19](#_Toc57021132)

[A) Intern 19](#_Toc57021133)

[B) Extern 21](#_Toc57021134)

[5.2 Anlage 2: Referenzdokumente 21](#_Toc57021135)

# Kapitel I Zweck des Dokuments

**Das Hauptziel** eines Business Continuity Plans (BCP) ist es, die Kontinuität der (Haupt-)Aktivitäten des Unternehmens im Falle eines Zwischenfalls, einer Krise oder einer Katastrophe zu gewährleisten.

**Wie?** Das betrifft:

1. **Antizipieren** und einen kohärenten Ansatz für die Umsetzung eines Business Continuity Plans annehmen, um die Hauptprozesse zu identifizieren und die Risiken zu analysieren, denen sie ausgesetzt sind
2. **Geeignete Verfahren zu entwickeln**, um zu wissen, wie auf einen Vorfall, eine Krise oder eine Katastrophe zu reagieren ist.
3. **Ermittlung der notwendigen Elemente** (Ausrüstung, Gebäude, Personal, sowohl intern als auch extern usw.), um die von der höchsten Ebene der Unternehmensführung validierten Verfahren zur Bewältigung von Vorfällen, Krisen und Katastrophen wirksam umzusetzen.

**Resultat?**

1. **Über die validierte Verfahren verfügen**
2. **Wissen, wie die Auswirkungen dieser Vorfälle** auf ein für das Unternehmen akzeptables Niveau **begrenzt werden können**.
3. **Definition von Zielen und Zeitspannen,** um die Kontinuität der (Haupt-)Aktivitäten des Unternehmens zu gewährleisten.

HINWEIS: Auch wenn die Verfahren validiert wurden, **vergessen Sie nicht, der Geschäftsleitung regelmäßig Bericht zu erstatten**, falls ein Vorfall eintritt, der sich auf die Kontinuität der Betriebsabläufe des Unternehmens auswirkt.

**Bedrohungen**: Das Kontinuitätsmanagement ist umfassender als mögliche IT-Vorfälle. Überschwemmungen oder Brände, die Abwesenheit von Mitarbeitern (Krankheit, Entlassung, Tod), das Verschwinden eines oder mehrerer für das Unternehmen wichtiger Lieferanten, Pandemie usw. kann auch die Kontinuität der Aktivitäten des Unternehmens gefährden. Bei der Organisation des Kontinuitätsmanagements, genauer gesagt bei der Risikobewertung, geht es darum, alle Arten von Bedrohungen zu identifizieren, die die Aktivitäten des Unternehmens bedrohen können, wobei auch das „Worst-Case-Szenario" berücksichtigt wird.

*Zur Identifizierung von Bedrohungen, Schwachstellen und Auswirkungen siehe Ihre Risikobewertung und Risikobehandlung.*

# Kapitel II Verbindungen zwischen den Verfahren

Das Diagramm (siehe unten) zeigt, wie sich der "Business Continuity Plan" mit anderen Verfahren integriert.

Um einen effektiven Business Continuity Plan zu haben, müssen Sie die Vorlagen zur Risikobewertung und Risikobehandlung ausgefüllt haben. Der Grad des Risikos und die Wahrscheinlichkeit eines Vorfalls hängt von der Risikobehandlung ab, die Sie durchgeführt haben. Die Bewältigung eines Vorfalls wird auch stark von den von Ihnen getroffenen Vorbeugungs- und Abhilfemaßnahmen abhängen.

**A**

Bei der Erstellung Ihres Business Continuity Plans und Ihres Incident Management Plans kann es notwendig sein, Ihre Risikobewertung zu aktualisieren (insbesondere, wenn Sie planen, die Risiken durch den Erwerb neuer Instrumente oder den Start neuer Projekte anzupassen).

**B**

Ihre Risikobeurteilung und Ihr Business Continuity Plan erfordert auch, dass Sie sich bei Ihren Lieferanten erkundigen, Ihre Verträge überprüfen und Ihren Lieferanten sogar bestimmte Service Level Agreements (SLAs) oder Klauseln auferlegen.

**C**

Die Kontinuität der Aktivitäten ist eng mit dem Management von Vorfällen verbunden, denn Sie müssen sicherstellen, dass Sie die Aktivitäten (zumindest die wesentlichen) des Unternehmens auch im Falle eines Vorfalls weiterführen können. Der Administrator des Business Continuity Plans sendet dem Administrator des Incident Management Plans die notwendigen Informationen, um Vorfälle zu managen.

**D**

**E**

Insbesondere können Sie über Ihre Kunden oder Lieferanten auf einen laufenden Vorfall aufmerksam werden.

Die meisten Vorfälle implizieren nicht unbedingt die Aktivierung des Business Continuity Plans, einfach weil es sich um „gewöhnliche" kleine Vorfälle handelt, die keine wirklichen Auswirkungen auf das Unternehmen haben. Wenn ein Vorfall mit Auswirkungen auf das Unternehmen eintritt, wird der Administrator des Business Continuity Plans, der den Business Continuity Plan aktiviert, benachrichtigt. Während des Vorfalls stellt der Administrator des Incident Management Plans eine regelmäßige Berichterstattung an den Administrator des Business Continuity Plans sicher. Nach dem Vorfall sendet der Administrator des Incident Management Plans den "Post Incident Review" an den Administrator des Business Continuity Plans.

**F**

Wenn der Vorfall die Kontinuität des Betriebs nicht beeinträchtigt, kann der Administrator des Incident Management Plans gegebenenfalls Kunden und Lieferanten warnen, dass sich das Unternehmen in einem kleineren Vorfall befindet.

**G**

Wenn der Vorfall Auswirkungen auf die Unternehmenskontinuität hat, wendet sich der Administrator des Business Continuity Plans erforderlichenfalls an Kunden und Lieferanten auf der Grundlage der von den funktionalen Diensten und dem Administrator des Incident Management Plans bereitgestellten Informationen.

**H**

Nach einem Vorfall kann der Post Incident Review darauf hindeuten, dass die Risikobewertung und die Risikobehandlung angepasst werden müssen.

**I**

Nach einem Vorfall kann der Post Incident Review darauf hindeuten, dass Sie die Verträge mit Ihren Lieferanten überprüfen müssen.

**J**

Nach der Bewältigung von Vorfällen müssen Sie möglicherweise Ihre Risikobewertung und Risikobehandlung überprüfen oder Ihren Business Continuity Plan verbessern. **Weitere Informationen zu den verschiedenen Verfahren finden Sie in den mitgelieferten Vorlagen.**

Damit der entwickelte Plan im Falle eines Vorfalls wirksam funktioniert, ist es wichtig, dass die geplanten **Verfahren im Voraus gründlich getestet und regelmäßig überprüft werden**. Denken Sie daran, Ihre Pläne mindestens einmal im Jahr und nach jedem Ereignis/jeder Krise oder Katastrophe zu überprüfen und „Lehren daraus zu ziehen", damit Sie Ihre Pläne auf der Grundlage der Bedürfnisse und Erfahrungen des Unternehmens verbessern können.

Jeder, der am Business Continuity Plan beteiligt ist, muss seine genaue Rolle kennen und die aktuellste Version des Plans haben. (Vergessen Sie nicht, auch eine Papierversion des Plans aufzubewahren).

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**3. Incident Management Plan**

**Essentielle   
Lieferanten**

**Kunden**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

# Kapitel III Wählen Sie jemanden, der am Ruder steht

## 3.1 Bestimmen Sie einen Administrator für den Business Continuity Plan

*"Everything that can go wrong will go wrong”*

*Murphy’s Law*

Der Vorfall kann an einem Freitagabend, einem Wochenende, am Tag vor einem Großauftrag oder während der Feiertage usw. auftreten.

Es ist daher besser, im Voraus über mögliche Vorfälle nachzudenken, als völlig unvorbereitet zu sein, wenn der Vorfall tatsächlich eintritt.

Denken Sie also daran, jemanden zu ernennen, der „am Ruder stehen wird", sowie eine weitere Person, die diese Person im Falle von Abwesenheit/Weggang/Krankheit ersetzen kann.

*Wen sollten sie wählen?* Im Idealfall sollte diese Person ein guter Kommunikator sein, das Unternehmen gut genug kennen, stressresistent sein und über ausreichende Erfahrung verfügen. In größeren Unternehmen kann ein „Team" ernannt werden.

Dies kann das Management sein oder jemand mit der Autorität, eine strategisch-operative Rolle zu übernehmen.

Hinweis: „Administrator" bedeutet nicht immer „verantwortlich", der Administrator muss unter Umständen auf mehrere interne Manager zurückgreifen, aber es versteht sich von selbst, dass wichtige Entscheidungen und die letztendliche Verantwortung bei der höchsten Führungsebene liegen. Es ist daher wichtig, dass alle Verfahren von der Geschäftsleitung validiert werden.

## 3.2 Rollen des Administrators des Business Continuity Plans

Der Administrator des Business Continuity Plans muss für einen konstruktiven Dialog innerhalb des Unternehmens sorgen, die Zusammenarbeit zwischen den beteiligten Abteilungen oder Personen fördern und die Berichterstattung an die Geschäftsleitung sicherstellen.

Der Administrator des Business Continuity Plans (je nach Größe und Bedarf des Unternehmens als Einzelperson oder als Teamleiter):

1. Stellt das Business Continuity Team (falls vorhanden) zusammen und kontaktiert den/die Schlüsselexperten (IT-Dienste, Sicherheits- und Präventionsberater, Datenschutzbeauftragter (DSB), Informationssicherheitsberater usw.)
2. Hält eine erste Besprechung ab (mit dem Business Continuity Team, falls vorhanden, und, falls nicht vorhanden, mit der Geschäftsleitung), um die Auswirkungen des Vorfalls zu beurteilen und den Grad der Kritikalität des Vorfalls und der betroffenen Aktivitäten zu bestimmen. (Es ist möglich, die Situation je nach den Umständen neu zu bewerten. Dies ist nur eine erste Beurteilung)
3. Informiert die Geschäftsleitung regelmäßig und erstattet ihm Bericht
4. Aktiviert den Business Continuity Plan
5. Identifiziert, wenn möglich, wie sich der Vorfall entwickeln könnte. Bestimmen Sie, welche Informationen noch fehlen, um die Situation besser zu verstehen, und wie diese Informationen innerhalb eines bestimmten Zeitrahmens gesammelt werden sollen (Anmerkung: Es geht nicht darum, in dieser Phase *alle* Informationen zu sammeln, sondern nur die dringendsten Informationen, d.h. was für eine erste Beurteilung des aktuellen und wahrscheinlichen Kritikalitätsgrades des Vorfalls erforderlich ist).
6. Kontaktiert die Kommunikations- und Kundenbeziehungsdienste (falls vorhanden) oder schlägt der Geschäftsleitung gegebenenfalls einen Kommunikationsplan in Bezug auf die Kunden und Lieferanten vor (siehe Blatt „Kommunikation").
7. Nimmt Kontakt mit den betroffenen Funktionsverantwortlichen auf und leitet die in dieser Phase gesammelten Informationen an sie weiter
8. Unterhält einen Dialog mit den beteiligten funktionalen Abteilungen und stellt während des gesamten Vorfalls die Berichterstattung auf Geschäftsleitungsebene sicher
9. Kann die Reduzierung oder Unterbrechung einer nicht wesentlichen Aktivität anordnen, um die notwendigen Ressourcen für die wesentlichen Aktivitäten zu erhalten
10. Kann sich um die Evakuierung von Mitarbeitern und Kunden kümmern
11. Kann mit Kunden und Lieferanten kommunizieren (externe Kommunikation)
12. Beendet die Aktivierung des Business Continuity Plans
13. Nimmt am (Post Incident Review) (NACH DEM VORFALL) teil
14. Gewährleistet die Revision der Pläne (mögliche Änderungen je nach Bedarf und Erfahrung) und die Validierung der Pläne durch die Geschäftsleitung
15. Organisiert die notwendigen Übungen und Tests, um das Bewusstsein zu erhöhen und den Business Continuity Plan zu aktualisieren
16. Hält die Pläne für Schlüsselpersonen bereit (auch auf Papier und außerhalb eines möglichen Überschwemmungsgebietes)
17. *... [identifizieren Sie eventuelle andere Rollen]*

NB: In einigen Unternehmen ist es möglich:

* dass *eine* Person oder ein Team die Verwaltung aller Vorfälle übernimmt.
* dass Außenstehende in den Prozess einbezogen werden. Zum Beispiel eine Anwaltskanzlei, externe Datenschutzbeauftragte, Versicherer usw.
* dass bestimmte Schritte nicht stattfinden (z. B. die Schritte 6 und 7).

# Kapitel IV BUSINESS CONTINUITY PLAN - GESCHÄFTSKONTINUITÄTSKONTINUITÄTSPLAN

*„In preparing for battle, I have always found that plans are useless, but planning is indispensable.”*

*General Dwight D. Eisenhower*

Es ist unmöglich, alles vorauszusehen, plötzliche und unvorhersehbare Ereignisse können immer eintreten.

Wenn ein Vorfall eintritt, hat Ihr Plan vielleicht nicht „an alles gedacht", aber die einfache Tatsache, dass Sie sich auf andere Arten von Vorfällen vorbereitet und begonnen haben, über die Unternehmenskontinuität nachzudenken, wird Ihnen helfen, widerstandsfähiger zu sein und zumindest die wesentlichen Aktivitäten Ihres Unternehmens weiterführen zu können.

Ein Geschäftskontinuitätsplan basiert auf 5 Schritten:

Schritt 1: Definition des Umfangs des Business Continuity Plans

Schritt 2: Aktivierung des Plans

Schritt 3: Deaktivierung des Plans

Schritt 4: Testen und halten Sie Ihren Plan auf dem Laufenden

## 4.1 Schritt 1: Anwendungsbereich des Business Continuity Plans:

Ein Business Continuity Plan ist ein iterativer (sich wiederholender) Prozess:

Konzentrieren Sie sich in einer ersten Iteration auf das Wesentliche: Welche Aktivitäten sind für das wirtschaftliche Überleben Ihres Unternehmens unerlässlich? Beachten Sie dabei insbesondere:

* wie viel des Umsatzes diese Aktivitäten generieren
* die Anzahl der Kunden für diese Aktivität
* die Auswirkungen, wenn die Aktivität reduziert oder eingestellt werden muss: Auswirkungen auf die Produktivität, die Finanzen und/oder den Ruf des Unternehmens.

Vielleicht möchten Sie Ihren Business Continuity Plan zunächst auf diese kritischen Aktivitäten beschränken.

NB: Ihre Risikoeinschätzung sollte Ihnen bereits in dieser Phase geholfen haben, die Dinge klarer zu sehen.

| Essentielle Aktivität 1 |
| --- |
| Liste der essentiellen Elemente zur Gewährleistung der Kontinuität der betreffenden wesentlichen Geschäftstätigkeit |
| Schlüsselperson |
| Wichtige Informationen oder Daten |
| Notwendige IT-Dienste (Hardware, Software) |
| Gebäude |
| … |

## 4.2 Schritt 2: Aktivierung des Plans

Der Administrator des Business Continuity Plans kann den Plan aktivieren, z.B. weil die Regierung oder die Aufsichtsbehörde des Sektors Maßnahmen zur Ordnung ergriffen hat, weil Lieferanten einen Mangel an einem wesentlichen Element angezeigt haben oder weil der Administrator des Incident Management Plans davor gewarnt hat, dass es Auswirkungen auf die Kontinuität der Aktivitäten des Unternehmens geben könnte.

|  |
| --- |
| **SAFETY FIRST: Schützen Sie zuerst Menschenleben!** |

Es versteht sich von selbst, aber bevor die Kontinuität der Aktivitäten des Unternehmens gewährleistet werden kann, geht es zunächst um den Schutz von Menschenleben. Dies bedeutet auch, dass je nach den Umständen des Unternehmens geeignete Maßnahmen ergriffen werden müssen.

Besondere Aufmerksamkeit muss den Risiken von Feuer, Explosion, Exposition gegenüber toxischen Produkten, Überflutung usw. gewidmet werden.

Der für den Business Continuity Plan verantwortliche Manager oder das Team führt die folgenden Kontrollen und/oder Maßnahmen durch, um das Wohlergehen der Menschen zu gewährleisten:

1. Identifizierung von Vorfallszenarien
2. Identifizierung der Arten von Risiken
3. Maßnahmen zur Gefahrenverhütung
4. Kontrollmaßnahmen
5. Anschließend Untersuchung des Vorfalls.

Diese Regelung ist identisch mit dem Incident Management Plan, der auch dem Administrator des Business Continuity Plans bekannt sein muss.

**Beispiel**

**Szenario:** Gefährliche Produkte laufen anormal ab oder verdunsten anormal, bewaffnete Personen betreten Gebäude, es gibt eine Epidemie oder Pandemie in der Region, in der sich die Arbeitsplätze befinden oder in deren Nähe, das Trinkwasser ist verunreinigt, ein Brand oder eine Überschwemmung bedroht die üblichen Arbeitsplätze (Brand in einem nahe gelegenen Gebäude, Nähe bereits überschwemmter und überschwemmungsgefährdeter Gebiete) usw.

**Risiken:** Risiken für das Personal, Verletzungen, Todesfälle und psychologische Folgen müssen berücksichtigt werden.

**Maßnahmen zur Gefahrenverhütung:**

* Ermitteln Sie den verbindlichen Rechtsrahmen (Kodex für gutes Wohlbefinden am Arbeitsplatz usw.) und konsultieren Sie die Website des [FÖD Beschäftigung](https://werk.belgie.be/nl/themas/welzijn-op-het-werk), die Website der [Europäischen Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz](https://oiraproject.eu/en/oira-tools) und des belgischen Wissenszentrums für Wohlbefinden am Arbeitsplatz ([BeSWIC](https://www.beswic.be/nl)).
* Einhaltung gesetzlicher und/oder behördlicher Verpflichtungen (Feueralarme, Brandschutztüren usw.).
* Identifizieren Sie die unentbehrlichen Experten und legen Sie vor jedem Vorfall Rollen und Verantwortlichkeiten fest.
* Identifizieren Sie die Notrufnummern und die Möglichkeiten, diese zu erreichen.
* Stellen Sie einen Defibrillator im Gebäude bereit
* Machen Sie das Personal auf bewährte Praktiken aufmerksam (auf dem Gelände nicht rauchen, keine Türen oder Fenster offen lassen, jeden Vorfall, der andere gefährden könnte, sofort melden, das Personal in grundlegender Erster Hilfe schulen usw.).
* Erstellen Sie Evakuierungspläne (Brand, Überschwemmung usw.) und testen Sie diese regelmäßig (mindestens einmal pro Jahr).
* Identifizieren Sie Personen, die einem höheren Risiko ausgesetzt sind (Bewegungs- und Atembeschwerden usw.) oder die besonders empfindlich sind (Herz- und Atembeschwerden usw.).

**Kontrollmaßnahmen**

Je nach dem Grad der Kritikalität des Vorfalls wird der Vorfall zunächst durch den Administrator des Incident Management Plan qualifiziert. Wenn die Gefahr besteht, dass die Aktivitäten des Unternehmens beeinträchtigt werden, informiert der Administrator des Incident Management Plans den Administrator des Business Continuity Plans. (NB: in kleineren Strukturen ist es möglich, dass ein und dieselbe Person diese verschiedenen Funktionen übernehmen kann).

Diese erste Bewertung ist schnell durchgeführt und muss möglicherweise im Laufe eines Vorfalls überprüft werden.

|  | Aktion | Wer macht was? | Verweise auf andere Dokumente |
| --- | --- | --- | --- |
|  | Beschreibung der Aktion | Funktionen und Rollen der für die Durchführung der Aktion verantwortlichen Schlüsselpersonen | Referenz zu anderen Dokumenten |
|  | Sensibilisierung für die gesetzlichen Verpflichtungen im Zusammenhang mit der Verhütung von Berufsrisiken und dem Schutz von Gesundheit und Sicherheit am Arbeitsplatz. |  |  |
|  | Besuchen Sie die Website von BESWIC  <https://www.beswic.be/nl>  Checklisten sind beim FÖD Beschäftigung je nach Art des befürchteten Ereignisses (Pandemie usw.) erhältlich.  Instrumente sind auch bei der Europäischen Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz erhältlich.  <https://oiraproject.eu/en/oira-tools> |  |  |
|  | Über angemessene Verfahren verfügen (Incident Management) |  |  |
|  | Definition von Rollen und Verantwortlichkeiten (vor einem Vorfall) |  |  |
|  | Identifizierung aller Kontrollmaßnahmen (siehe Incident Management) |  |  |
|  | Ermittlung und Pflege einer Liste von Notfalldiensten und internen und externen Kontakten. |  |  |
|  | Informieren Sie die Mitarbeiter und möglicherweise externe Interessenvertreter (Kunden, Lieferanten) darüber, dass ein Vorfall stattfindet und dass Maßnahmen zu dessen Bewältigung ergriffen werden. |  |  |
|  | Führen von Ereignisprotokollen (Protokolle, Beweise, Spuren) |  |  |
|  | Erwägen Sie die regelmäßige Kontaktaufnahme mit den (Familien von) möglichen Verletzten. |  |  |
|  | … |  |  |

## 4.3 Schritt 3: Führen Sie die zu ergreifenden Aktionen auf

Vergessen Sie Ihre Risikobewertung und Risikobehandlung nicht: Sie haben bereits viele Schritte unternommen, um das Risiko zu verringern oder die Auswirkungen eines Vorfalls zu begrenzen. Wenn Sie bei der Entwicklung Ihres Business Continuity Plans andere Maßnahmen in Betracht ziehen, vergessen Sie nicht, Ihre Risikobewertung und Risikobehandlung auf dem neuesten Stand zu halten. Der Business Continuity Plan ist auch mit dem Incident Management Plan verknüpft (siehe Vorlage Incident Management).Der Administrator oder das Team des Business Continuity Plan wird die notwendigen Schritte unternehmen, um den durch den Vorfall verursachten Schaden zu begrenzen und zu minimieren und die wesentlichen Aktivitäten aufrechtzuerhalten. Eines der Dinge, die Sie tun können, wenn Sie Ihren Business Continuity Plan schreiben, ist die Entwicklung von Checklisten. Beachten Sie jedoch, dass es unmöglich ist, alle Vorfallszenarien zu identifizieren, und dass es viel wichtiger ist, dass das Team in der Lage ist, sich an die Umstände anzupassen. Sobald das betroffene Personal von diesen Plänen Kenntnis hat, wird das Unternehmen besser in der Lage sein, auf jeden Vorfall zu reagieren, der eintreten könnte.

*Bitte füllen Sie diese Tabelle entsprechend der Situation Ihres Unternehmens aus:*

| **Aktion** | **Wer macht was?** | **Verweise auf andere Dokumente** |  |
| --- | --- | --- | --- |
| Beschreibung der Aktion | Funktionen und Rollen der für die Durchführung der Aktion verantwortlichen Schlüsselpersonen | Referenz zu anderen Dokumenten | OK? |
| Identifizieren der wichtige Prozesse und Aktivitäten, die gestört sind, und beschreiben Sie die Auswirkungen auf die Dienstleistung. |  |  |  |
| Identifizieren der (Risiken von) Schäden, sowohl materieller als auch immaterieller Art (z.B. Reputation). |  |  |  |
| Aktionen festlegen, um sicherzustellen, dass sich die Situation nicht verschlechtert.   * Lassen Sie diese Entscheidungen von der Geschäftsleitung validieren |  |  |  |
| Identifizieren, was intakt ist („was noch funktioniert") |  |  |  |
| Aktionen zur Mobilisierung zusätzlicher Ressourcen, sowohl durch eigenes Personal als auch durch Unterauftragnehmer.   * Lassen Sie diese Entscheidungen von der Geschäftsleitung validieren |  |  |  |
| … |  |  |  |

#### Szenario: Das Hauptgebäude ist nicht zugänglich

| Element  (Beschreibung) | Schaden  (Beschreibung) | Aktionen und Anweisungen | Geschätzte Wiederherstellungszeit |
| --- | --- | --- | --- |
| Z. B. Nationaler Streik, der den Zugang zu Ihrem Hauptgebäude blockiert.  Z. B. Unterbrechung oder Abschaltung der Stromversorgung, die den Zugang unmöglich oder schwierig macht. | Identifizieren der wichtige Prozesse und Aktivitäten, die gestört sind, und Beschreibung der Auswirkungen auf die Dienstleistung.  Identifizieren der (Risiken von) Schäden, sowohl materieller als auch immaterieller Art (z.B. Reputation).  Identifizieren, was intakt ist („was noch funktioniert") | (Erstellung einer Liste von Präventivmaßnahmen *(im Zusammenhang mit dem Risk Treatment und Incident Management Plan)*  Aufstellung der Liste der Kontrollmaßnahmen  *Aktionen festlegen, um sicherzustellen, dass sich die Situation nicht weiter verschlechtert.*  *Aktionen zur Mobilisierung zusätzlicher Ressourcen, sowohl durch eigenes Personal als auch durch Unterauftragnehmer identifizieren.*  So werden z.B. Beschäftigte auf Telearbeit gesetzt (für diejenigen, die nicht streiken), Lieferanten gewarnt, nicht an die übliche Adresse zu liefern, Kunden gewarnt, nicht ins Hauptgebäude zu gehen und mögliche Konsequenzen für die Lieferzeiten angegeben.  Wenden Sie sich z.B. an den Elektriker oder den Netzbetreiber (siehe auch die obigen Maßnahmen). | Z. B. 1 Tag, 1 Woche  Z. B. 4 Stunden oder 1 Woche usw. |
| … |  |  |  |

#### Szenario: Unterbrechung der Verbindung mit der Cloud oder dem Rechenzentrum

| Element  (Beschreibung) | Schaden  (Beschreibung) | Aktionen und Anweisungen | Geschätzte Wiederherstellungszeit |
| --- | --- | --- | --- |
| Ihr Unternehmen hat keinen Zugriff mehr auf Daten und Dateien, die nicht lokal gespeichert sind usw. | Identifizierung der wesentlichen Aktivitäten (siehe Schritt 1), die betroffen sind, und Beschreibung der Auswirkungen auf diese Aktivitäten. | (Erstellung einer Liste von Präventivmaßnahmen *(im Zusammenhang mit dem Risk Treatment und Incident Management Plan)*  Z. B. mindestens eine lokale Kopie behalten usw.  Aufstellung der Liste der Kontrollmaßnahmen  Aktionen festlegen, um sicherzustellen, dass sich die Situation nicht verschlechtert.  *Aktionen festlegen, um sicherzustellen, dass sich die Situation nicht weiter verschlechtert.*  *Aktionen zur Mobilisierung zusätzlicher Ressourcen, sowohl durch eigenes Personal als auch durch Unterauftragnehmer identifizieren.*  Wenden Sie sich z. B. an den Cloud-Provider oder den Rechenzentrumsmanager und bestimmen Sie die geschätzte Wiederherstellungszeit, lassen Sie sich in Echtzeit informieren.  Wenden Sie z. B. die Vertragsstrafen für die Nichteinhaltung des vereinbarten Servicelevels (SLA) an. | Z. B. 5 Stunden bis zu 2 Tagen |

#### Szenario: Überschwemmung

| Element  (Beschreibung) | Schaden  (Beschreibung) | Aktionen und Anweisungen | Geschätzte Wiederherstellungszeit |
| --- | --- | --- | --- |
| Eine Überschwemmung | Identifizierung der wesentlichen Aktivitäten (siehe Schritt 1), die betroffen sind, und Beschreibung der Auswirkungen auf diese Aktivitäten. | (Erstellung einer Liste von Präventivmaßnahmen *(im Zusammenhang mit dem Risk Treatment und Incident Management Plan)*  SIEHE FICHE ÜBERSCHWEMMUNG  Aufstellung der Liste der Kontrollmaßnahmen  *Aktionen festlegen, um sicherzustellen, dass sich die Situation nicht weiter verschlechtert.*  *Aktionen zur Mobilisierung zusätzlicher Ressourcen, sowohl durch eigenes Personal als auch durch Unterauftragnehmer identifizieren.*  Z.B.: Telearbeit für Mitarbeiter, Kontakt mit Versicherungen, manuelle oder pneumatische Evakuierung des modderigen Wassers usw. | Z. B. 1 Woche |

#### Szenario: ...

| Element  (Beschreibung) | Schaden  (Beschreibung) | Aktionen und Anweisungen | Geschätzte Wiederherstellungszeit |
| --- | --- | --- | --- |
| ..... |  | ... | …. |

## 4.4 Schritt 4: Deaktivierung des Business Continuity Plan

Die Deaktivierung des Business Continuity Plan wird vom Verwalter des Geschäftskontinuitätsplans in Absprache mit der Geschäftsleitung vorgenommen.

Insbesondere kann der Business Continuity Plan deaktiviert werden, wenn der Vorfall abgeschlossen ist oder wenn es keine/keine weiteren Auswirkungen auf die wesentlichen Aktivitäten des Unternehmens gibt (auch wenn der Vorfall noch andauert, z.B. weil eine vorübergehende Lösung gefunden wurde).

| **Kriterien für die Aktivierung des Business Continuity Plans** |
| --- |
| Sind alle Dienstleistungsniveaus wieder auf das normale oder das akzeptable Mindestniveau zurückgekehrt? |
| Gibt es irgendeinen Grund, daran zu zweifeln, dass das Dienstleistungsniveau in den kommenden Tagen stabil erreicht wird? |
| Wurden die Kontrollmaßnahmen (einschließlich vorübergehender Lösungen) deaktiviert? |
| Sind die Einsatzteams (funktionale Dienste) ausreichend ausgerüstet, um mit möglichen Folgen nach einem Vorfall umzugehen? |
| Hat die endgültige Kommunikation mit externen Parteien (Kunden, Lieferanten usw.) stattgefunden? |
| ... |

Im Rahmen der Deaktivierung des Business Continuity Plans müssen die Ereignisse beschrieben werden, damit die nächste Aktivierung des Plans verbessert werden kann.

| **Aktion** | **Wer macht was?** | **Verweise auf andere Dokumente** |
| --- | --- | --- |
| Kurze Beschreibung der genommenen Aktionen (Kontrollmaßnahmen) |  |  |
| Verweisen Sie auf den Post Incident Review |  |  |
| Kontaktieren Sie den Versicherer |  |  |
| Richten Sie eine "Endvorfall/-krisen"-Kommunikation zuhanden der beteiligten externen Personen (Kunden, Lieferanten) ein. |  |  |
| Feststellen, ob es Bereiche des Business Continuity Plan gibt, die verbessert werden könnten (einschließlich externer Vertragsbeziehungen). |  |  |
| Anwendung möglicher Vertragsstrafen im Falle der Nichteinhaltung von Service Levels (SLAs). |  |  |

**Das Post Incident Review**

Es geht jetzt darum, den Bericht zur Deaktivierung des Business Continuity Plan um den Post Incident Review zu ergänzen. (Siehe Incident Management Plan und die Fiches).

## 4.5 Schritt 5: Testen Sie Ihren Plan und halten Sie ihn auf dem Laufenden

„***Ein Plan, der in einem Regal schläft, ist das Papier nicht wert, auf dem er gedruckt ist."***

Denn wenn der Business Continuity Plan verstaubt, besteht die Möglichkeit, dass im Falle eines Vorfalls niemand weiß, wie er anzuwenden ist. Eine regelmäßige Sensibilisierung ist notwendig.

Denken Sie daran, das Personal zu schulen und denken Sie über die verschiedenen Kommunikationskanäle nach (Plakate, Beschilderung, Übungen, Hilfsmittel). Für Ideen zu Werkzeugen siehe: [BeSWIC](https://www.beswic.be/fr/en-pratique/loutil-dinstruction-toworksafe-pour-la-securite-des-travailleurs-allophones) (FR) zur Mitarbeitersicherheit; [Cyber Security Coalition](https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/) (FR) zur Cybersicherheit; [SPF](https://emploi.belgique.be/fr/actualites/coronavirus-materiel-de-sensibilisation-sur-le-lieu-de-travail-en-17-langues) Emploi (FR) zu Pandemien usw.

|  |  |  |
| --- | --- | --- |
| **Maßnahmen** | **Anmerkungen** | **OK?** |
| Benennung eines Administrators plus eine Vertretung für den Fall seiner Abwesenheit  oder  Weisen Sie ein Team zu, das für den Business Continuity Plan verantwortlich sein wird (plus einen Leiter) |  |  |
| Stellen Sie sicher, dass das Personal mindestens einmal im Jahr und bei wichtigen Aktualisierungen geschult wird. |  |  |
| Organisieren Sie regelmäßig eine Übung (mindestens einmal pro Jahr) |  |  |
| Stellen Sie die notwendigen Kontakte (Lieferanten, Rechtsanwälte, Versicherer usw.) zur Verfügung und überprüfen Sie die Aktualität der Kontakte (mindestens einmal pro Jahr). |  |  |
| Testen Sie die Datensicherungs- und Wiederherstellungsverfahren regelmäßig (idealerweise vierteljährlich). |  |  |
| Aktualisieren Sie den Business Continuity Plan entsprechend den Personen (Ankunft/Austritt) und Umständen (neue Projekte, neues Management der internen Verfahren usw.). |  |  |

# Kapitel V Anlagen

## 5.1 Anlage 1: Kontaktliste

### A) Intern

#### Schlüsselmitarbeiter

| Rolle | Vorname und NAME | Funktion | Kontaktangaben  Geben Sie mindestens 2 Ansprechpartner pro Rolle an (1 Hauptansprechpartner und 1 Ansprechpartner im Falle von Krankheit, Urlaub, Ausscheiden des Hauptansprechpartners) |
| --- | --- | --- | --- |
| Leiter des Business Continuity Teams oder Administrator des Business Continuity Plans |  |  | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| Mitglieder des Business Continuity Plan Teams |  |  | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| Funktionaler Dienst 1 |  | Essentielle Aktivitäten (identifizier) | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| Funktionaler Dienst 2 |  | Essentielle Aktivitäten (identifizier) | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| … |  |  |  |

### B) Extern

#### Lieferanten, Kunden usw.

| Rolle | Name des Unternehmens  Vorname und NAME des Ansprechpartners | Referenz zu Vertrag/Verträgen | Kontaktangaben  Geben Sie mindestens 2 Ansprechpartner pro Rolle an (1 Hauptansprechpartner und 1 Ansprechpartner im Falle von Krankheit, Urlaub, Ausscheiden des Hauptansprechpartners) |
| --- | --- | --- | --- |
| Lieferant 1 |  |  | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| Kunde 1 |  |  | Hauptansprechpartner  @  T  M  Andere  @  T  M |
| ... |  |  |  |

## 5.2 Anlage 2: Referenzdokumente

1. Risk Assessment & Treatment
2. Incident Management Plan
3. Krisenmanagementplan
4. …