Incident   
Response Plan

Incident   
Response Plan

Dokument: Verlauf

**Versionsverlauf des Dokuments**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Geändert von** | **Geänderte Elemente (V +1)** |
| **xxx** | **xxx** | **xxx** | **xxx** |

**Verlauf der Bestätigungen**

|  |  |  |
| --- | --- | --- |
| **Name** | **Funktion** | **Datum der Bestätigung durch die höchste Geschäftsführungsebene** |
| **xxx** | **xxx** | **xxx** |

Das vorliegende Dokument gilt ab [Datum].

Dieses Dokument wird folgendermaßen aufbewahrt:

* Als Papierversion an folgenden Stellen: [Orte angeben].
* In digitaler Form an folgenden Stellen: [z. B. Speicherort im Intranet].

Der Inhaber dieses Dokuments ist [Funktion]. Er prüft mindestens einmal jährlich, ob Aktualisierungen notwendig sind

**INHALTSVERZEICHNIS**

[Incident Response Plan 1](file:////Users/kris/Downloads/DUITS%20na%20te%20kijken/IRP%20grandes%20structures_DU.docx#_Toc58459795)

[Incident Response Plan 1](file:////Users/kris/Downloads/DUITS%20na%20te%20kijken/IRP%20grandes%20structures_DU.docx#_Toc58459796)

[Dokument: Verlauf 2](#_Toc58459797)

[Versionsverlauf des Dokuments 2](#_Toc58459798)

[Verlauf der Bestätigungen 2](#_Toc58459799)

[**Kapitel I.** Zweck des Dokuments 4](#_Toc58459800)

[**Kapitel II.**  Verbindungen zwischen den Verfahren 5](#_Toc58459801)

[**Kapitel III.**  Rollen 8](#_Toc58459802)

[3.1 Helpdesk 8](#_Toc58459803)

[3.2 Vorfallmanagementteam (Incident-Management-Team) 9](#_Toc58459804)

[3.3 Geschäftskontinuitätsteam (Business-Continuity-Team) 9](#_Toc58459805)

[3.4 Krisenmanagementteam (Crisis Management Team) 9](#_Toc58459806)

[**Kapitel IV.** INCIDENT RESPONSE PLAN 10](#_Toc58459807)

[4.1 Schritt 1: Vorbereitung 11](#_Toc58459808)

[4.2 Schritt 2: Benachrichtigung und Identifizierung 11](#_Toc58459809)

[4.2.1. Niedrig 11](#_Toc58459810)

[4.2.2. Geringfügig 12](#_Toc58459811)

[4.2.3. Hoch 12](#_Toc58459812)

[4.2.4. Krise 13](#_Toc58459813)

[4.3 Schritt 3: Aktivierung und Verarbeitung 14](#_Toc58459814)

[4.4 Schritt 4: Beseitigung 14](#_Toc58459815)

[4.5 Schritt 5: Deaktivierung 15](#_Toc58459816)

[4.6 Schritt 6: Erkenntnisse (Post Incident Review) 15](#_Toc58459817)

[**Kapitel V.** Anhänge 19](#_Toc58459818)

[5.1. Anhang 1. Kontaktliste 19](#_Toc58459819)

[A) Intern 19](#_Toc58459820)

[B) Extern 21](#_Toc58459821)

[5.2. Anhang 2: Referenzdokumente 21](#_Toc58459822)

Kapitel I.  
Zweck des Dokuments

**Das Hauptziel** des Incident Response Plans ist es, im Voraus festzulegen, wie Ihr Unternehmen mit derartigen Vorfällen umgehen wird, um Schäden und Risiken im Hinblick auf eine Fortführung Ihrer wesentlichen Aktivitäten zu reduzieren.

Dieser Incident Response Plan legt die empfohlene Organisation, Maßnahmen und Verfahren fest im Hinblick auf:

* das Erkennen eines Vorfalls und die entsprechende Reaktion
* eine schnelle und effektive Einschätzung der Situation
* die Benachrichtigung der relevanten Personen und Organisationen über den Vorfall
* die Organisation von Aktivitäten zur Reaktion des Unternehmens, einschließlich der Aktivierung einer Kommandozentrale
* eine Beschleunigung der Reaktionsbemühungen des Unternehmens auf der Grundlage der Schwere des Vorfalls und
* das Einleiten, falls erforderlich, von Bemühungen zur Wiederherstellung des Unternehmens nach dem Vorfall.

Dieser Plan setzt voraus, dass das Unternehmen bereits eine Risikobewertung (Risk Assessment) und Risikobehandlung (Risk Treatment) abgeschlossen hat.

Kapitel II.   
Verbindungen zwischen den Verfahren

Das Diagramm (siehe unten) zeigt, wie sich der Incident Response Plan in andere Verfahren einfügt.

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**Hauptlieferanten**

**Kunden**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

**3. Vorfallmanagement  
IRP  
CMP  
DRP**

1. Ein effektives Vorfallmanagement setzt voraus, dass das Unternehmen die Vorlagen zur Risikobewertung und Risikobehandlung bereits ausgefüllt hat. Die Höhe des Risikos und die Wahrscheinlichkeit eines Zwischenfalls hängen von der Risikobehandlung ab, die Sie durchgeführt haben. Das Vorfallmanagement und der Business Continuity Plan hängen sehr stark von den präventiven und kurativen Maßnahmen ab, die Sie ergreifen.
2. Bei der Erstellung Ihres Geschäftskontinuitätsplans und Ihres Business Continuity Plans müssen Sie möglicherweise Ihre Risikobewertung aktualisieren (insbesondere, wenn Sie planen, Risiken durch den Erwerb neuer Ausrüstung oder den Start neuer Projekte zu ändern).
3. Ihre Risikobewertung und Ihr Geschäftskontinuitätsplan setzen ebenfalls voraus, dass Sie sich bei Ihren Lieferanten erkundigen, Ihre Verträge überprüfen und Ihren Lieferanten sogar bestimmte Dienstgütevereinbarungen (Service Level Agreements; SLA) oder Klauseln auferlegen.
4. Die Aufrechterhaltung des Geschäftsbetriebs ist eng mit dem Vorfallmanagement verknüpft, da Sie sicherstellen müssen, dass Sie auch im Falle eines Zwischenfalls die (zumindest wesentlichen) Aktivitäten des Unternehmens weiterführen können. Der Leiter des Geschäftskontinuitätsplans leitet die erforderlichen Informationen an den Leiter des Business Continuity Plans weiter.
5. Sie könnten insbesondere über Ihre Kunden oder Lieferanten auf einen aktuellen Vorfall hingewiesen werden.
6. Die meisten Zwischenfälle erfordern nicht zwangsläufig die Aktivierung des Business Continuity Plan, weil es sich schlicht um „gewöhnliche“ kleine Zwischenfälle handelt, die keine weitreichenden Auswirkungen auf die Geschäftstätigkeit haben. Wenn ein Vorfall mit Auswirkungen auf den Geschäftsbetrieb eintritt, benachrichtigt der Vorfallmanager den Leiter des Geschäftskontinuitätsplans, der den Business Continuity Plan aktiviert. Während des Vorfalls sorgt der Vorfallmanager für eine regelmäßige Berichterstattung an den Leiter des Kontinuitätsplans. Nach dem Vorfall sendet der Vorfallmanager die „Post Incident Review“ an den Leiter des Kontinuitätsplans.
7. Wenn der Vorfall keine Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs hat, kann der Leiter des Business Continuity Plans gegebenenfalls Kunden und Lieferanten benachrichtigen, dass im Unternehmen ein kleinerer Vorfall eingetreten ist.
8. Wenn der Vorfall Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs hat, wendet sich der Leiter des Geschäftskontinuitätsplans gegebenenfalls an Kunden und Lieferanten entsprechend den von den betrieblichen Diensten und dem Leiter des Business Continuity Plans erhaltenen Informationen.
9. Nach einem Vorfall kann die „Post Incident Review“ darauf hindeuten, dass Risikobewertung und Risikobehandlung geändert werden sollten.
10. Nach einem Vorfall kann die „Post Incident Review“ darauf hindeuten, dass Sie die Verträge mit Ihren Lieferanten überprüfen sollten.

Nach dem Vorfallmanagement müssen Sie möglicherweise Ihre Risikobewertung (Risk Assessment) und Risikobehandlung (Risk Treatment) überprüfen oder Ihren Geschäftskontinuitätsplan (BCP) verbessern. **Weitere Informationen zu den verschiedenen Verfahren finden Sie in den mitgelieferten Vorlagen.**

Alle am Geschäftskontinuitätsplan (BCP) beteiligten Personen müssen ihre genaue Rolle kennen und über die aktuellste Version des Plans verfügen. (Denken Sie daran, auch eine Papierversion aufzubewahren).

1. Der Leiter des Incident Response Plan (IRP) benachrichtigt den Leiter des Crisis Management Plan (CMP), dass ein die Aufrechterhaltung des Geschäftsbetriebs beeinträchtigender Vorfall sich (vermutlich) ereignet. Der Leiter des Crisis Management Plan informiert den Leiter des IRP und kann sich auf ihn verlassen.
2. Der Leiter des Crisis Management Plan (CMP) benachrichtigt den Leiter des Geschäftskontinuitätsplans (BCP).
3. Der Leiter des Crisis Management Plan (CMP) konsultiert und informiert den Leiter des Geschäftskontinuitätsplans (BCP).
4. Der Leiter des Crisis Management Plan (CMP) benachrichtigt den Leiter des Notfallplans zur Wiederherstellung des Betriebs (Disaster Recovery Plan; DRP).
5. Der Leiter des Notfallplans zur Wiederherstellung des Betriebs konsultiert und informiert den Leiter des Business Continuity Plans.
6. Die Leiter des Business Continuity Plan (BCP) und des Disaster Recovery Plan (DRP) halten sich gegenseitig über die Entwicklungen auf dem Laufenden.
7. Der Leiter des Incident Response Plans (IRP) informiert den Leiter des Business Continuity Plan (BCP) (ohne den Leiter des Crisis Management Plan zu benachrichtigen). Der Leiter des Business Continuity Plan (BCP) kann sich auf das Fachwissen des Vorfallreaktionsteams stützen.

**Incident Response Plan (IRP)**

**Crisis Management Plan (CMP)**

**Disaster Recovery Plan (DRP)**

**Business Continuity Plan (BCP)**

**6**

**7**

**1**

**4**

**5**

2

**3**

Damit der Business Continuity Plan (BCP) im Falle eines Zwischenfalls effektiv funktioniert, ist es wichtig, die **geplanten** Verfahren **im Vorfeld gründlich** zu testen **und regelmäßig zu überarbeiten**. Überarbeiten Sie mindestens einmal im Jahr und nach jedem Vorfall/jeder Krise oder Katastrophe Ihre Pläne und ziehen Sie Lehren daraus, damit Sie die Pläne ausgehend von den Bedürfnissen und Erfahrungen des Unternehmens verbessern können.

Kapitel III.   
Rollen

Die verschiedenen Rollen und Verantwortlichkeiten sind so zu beschreiben, dass jeder die ihm zugewiesene Rolle kennt.

### 3.1 Helpdesk

Das „Helpdesk“ oder die für Vorfälle zuständige Abteilung ist dafür verantwortlich, mit Hilfe geeigneter Hilfsmittel (Software) angemessene Verfahren zur Erfassung von Vorfällen einzurichten.

| **Funktion** | **Rollen** |
| --- | --- |
| Leiter des Helpdesk-Teams  (Helpdesk-Manager) | * Überwachung der Dienstgütevereinbarungen (Service Level Agreements; SLA) * ggf. Weiterleitung von Informationen an den Leiter des Business Continuity Plans |
| Helpdesk-Mitarbeiter  (Helpdesk-Operator) | * Erfassen der Vorfälle und Zuweisung von Prioritäten * Lösen der Vorfälle an vorderster Front gemäß definierter Verfahren * Informieren des Leiters des Helpdesk-Teams |
| usw. |  |

### 3.2 Vorfallmanagementteam (Incident-Management-Team)

Das Vorfallmanagementteam ist für die Ausführung des Incident Response Plans für Vorfälle mit Auswirkung auf die Geschäftsprozesse verantwortlich.

| **Funktion** | **Rollen** |
| --- | --- |
| Leiter des Vorfallmanagementteams  (Incident Response Manager) | * Ausarbeitung und Ausführung des Incident Response Plans für bestimmte Szenarien. * Überwachung laufender Vorfälle. * Benachrichtigung des Leiters des Crisis Management Plan (CMP) bzw. des Leiters des Geschäftskontinuitätsplans (BCP). |
| Mitglied des Vorfallmanagementteams  (Incident Response Team) | * Initiative zur Lösung kleinerer oder größerer Zwischenfälle auf der 2. bzw. 3. Ebene. * Interaktion mit an der Lösung von Zwischenfällen beteiligten Teams. |
| usw. |  |

### 3.3 Geschäftskontinuitätsteam (Business-Continuity-Team)

Das Geschäftskontinuitätsteam verwaltet die Ausführung des Business-Continuity-Plans für den Fall, dass sich ein Vorfall auf die Geschäftsprozesse auswirkt. Die Rollen und Verantwortlichkeiten des Business-Continuity-Teams sind im Business Continuity Plan (BCP, siehe Vorlage) definiert.

### 3.4 Krisenmanagementteam (Crisis Management Team)

Das Krisenmanagementteam ist für die Leitung des Crisis Management Plan und die damit verbundenen Verfahren verantwortlich. Es ist für die Koordination und Kommunikation im Katastrophenfall verantwortlich. Die Rollen und Verantwortlichkeiten des Krisenmanagementteams sind im Crisis Management Plan festgelegt.

Kapitel IV.  
INCIDENT RESPONSE PLAN

Der Incident Response Plan beruht auf sechs Schritten:

### 4.1 Schritt 1: Vorbereitung

Siehe auch Risk Assessment und Risk Treatment.

Ziehen Sie bei der Ausarbeitung Ihres Incident Response Plans insbesondere folgende Elemente in Betracht:

* Umgang mit dem Vorfall (Identifizierung, Eindämmung, Beseitigung und Wiederaufnahme von Aktivitäten nach dem Vorfall)
* Überwachung, Erkennen, Analyse und Meldung von Ereignissen und Vorfällen
* Aufzeichnung von Vorfällen
* Auswertung von Ereignissen und Entscheidungen und Entscheidungsfindung
* Auswertung von Schwachstellen bei Informationssicherheit bzw. Datenschutz
* Eskalation von Vorfällen (an das Business-Continuity-Team oder das Krisenmanagementteam)
* Wiederherstellung des Normalzustands nach Zwischenfällen
* Zeitpunkt, Inhalt und Adressaten der Kommunikation

### 4.2 Schritt 2: Benachrichtigung und Identifizierung

Es ist wichtig, einen Vorfall schnell erkennen, identifizieren und kennzeichnen/klassifizieren zu können, um seine Auswirkungen auf die Geschäftskontinuität durch die Aktivierung des entsprechenden Verfahrens einzudämmen. Der Mitarbeiter, der die Benachrichtigung über einen Vorfall erhält, kennzeichnet den Vorfall auf der Grundlage vorgegebener Kriterien.

Jeder Mitarbeiter muss jegliche Vorfälle oder Ereignisse, die zu einem Vorfall führen könnten, schnellstmöglich melden. Auch Kunden und Lieferanten können einen Vorfall melden.

Die Mittel zur Meldung von Vorfällen werden im Verfahren des Vorfallmanagements beschrieben.

Der Mitarbeiter, der die Informationen erhält (z. B. Helpdesk), muss diese beispielsweise folgendermaßen klassifizieren:

1. **Niedrig** - Es sind keine Zwischenfälle aufgetreten, aber das Ereignis im Zusammenhang mit einem System, einem Prozess oder einer Organisation kann das Auftreten eines Zwischenfalls in naher oder ferner Zukunft auslösen.

2. **Geringfügig** - Ein Vorfall, der keine wesentlichen Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs hat.

3. **Hoch** - Ein Vorfall, der erhebliche Auswirkungen auf die Organisation haben kann, jedoch noch nicht als Krise eingestuft wird.

4. **Krise** - Ein Vorfall, der erhebliche Auswirkungen auf die Organisation und die Aufrechterhaltung des Geschäftsbetriebs haben kann.

### 4.2.1. Niedrig

Bei der Aufzeichnung von Informationen zu Schwachstellen oder Ereignissen analysiert der verantwortliche Mitarbeiter die Informationen, ermittelt wenn möglich die Ursache und schlägt, falls erforderlich, Präventiv- und Korrekturmaßnahmen vor.

### 4.2.2. Geringfügig

Werden geringfügige Vorfälle identifiziert oder gemeldet, muss der verantwortliche Mitarbeiter:

1. Maßnahmen zur Eindämmung des Vorfalls ergreifen
2. den Vorfall gemäß dem anwendbaren Verfahren aufzeichnen und den Schweregrad gemäß den definierten Servicelevels und Schwellenwerten bewerten
3. die Ursache des Vorfalls analysieren
4. Korrekturmaßnahmen zur Beseitigung der Ursache des Vorfalls ergreifen (wenn möglich, innerhalb des für die Lösung vereinbarten Zeitrahmens)
5. die von dem Vorfall betroffenen oder in ihn verwickelten Personen über die Lösung informieren.

### 4.2.3. Hoch

Werden größere Vorfälle identifiziert oder gemeldet, muss der verantwortliche Mitarbeiter:

1. Maßnahmen zur Eindämmung des Vorfalls ergreifen
2. den Schweregrad gemäß den definierten Servicelevels und Schwellenwerten bewerten Ein geringfügiger Vorfall kann sich zu einem größeren Vorfall ausweiten, wenn die zur Lösung benötigte Zeit die vereinbarten Servicelevel überschreitet oder die Auswirkungen weiter zunehmen.
3. alle verantwortlichen Beteiligten über den Vorfall informieren, der sich in deren Verantwortungsbereich ereignet hat, und den voraussichtlichen Zeitrahmen für die Lösung angeben (siehe Geschäftskontinuitätsplan und Crisis Management Plan).
4. das für die Reaktion auf Zwischenfälle geeignete Team zusammenstellen.
5. den Fortschritt des Vorfalls überwachen und sich über den Status des Vorfallmanagements informieren.
6. die Ursache des Vorfalls analysieren
7. Korrekturmaßnahmen zur Beseitigung der Ursache des Vorfalls ergreifen.
8. die von dem Vorfall betroffenen oder in ihn verwickelten Personen über die Lösung informieren.
9. Wenn der größere Vorfall nicht innerhalb des Zeitrahmens gelöst wird, könnte er nach dem im Crisis Management Plan beschriebenen Eskalationsverfahren zu einer Krisensituation eskalieren.

Wenn der Vorfall nicht innerhalb des festgelegten Zeitrahmens gelöst werden kann, benachrichtigt der Leiter des Vorfallreaktionsteams unverzüglich das Business-Continuity-Team bzw. das Krisenmanagementteam, um zu beurteilen, ob der Geschäftskontinuitätsplan bzw. der Crisis Management Plan aktiviert werden muss.

| **Maßnahme** | **Funktion** | **Verbindungen zu anderen Dokumenten**  **Name und Referenz** |
| --- | --- | --- |
| Regelmäßiges Informieren des Krisenmanagers über die Situation und die voraussichtliche Wiederanlaufdauer. | Vorfallmanager an den Leiter des Crisis Management Plan | Crisis Management Plan |
| Regelmäßige Bewertung des voraussichtlichen Zeitpunkts der Wiederaufnahme; überschreitet dieser die festgelegte Wiederanlaufdauer (Recovery Time Objective, RTO), muss der Vorfall an das Business-Continuity-Team eskaliert werden. | Vorfallmanager an den Leiter des Geschäftskontinuitätsplans | Business Continuity Plan |
| usw. |  |  |

### 4.2.4. Krise

Im Krisenfall wird der Crisis Management Plan herangezogen (siehe Crisis Management Plan).

**Aufzeichnung von Vorfällen**

**Unabhängig von der Einstufung des Vorfalls ist für die Dauer des Vorfalls ein Vorfallprotokoll zu führen.**

**Die für die Verwaltung des Vorfalls verantwortliche/n Person/en muss/müssen alle ergriffenen Maßnahmen in einem Vorfallprotokoll festhalten.**

**Die nachstehende Tabelle kann als Vorlage für das Vorfallprotokoll verwendet werden:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Datum** | **Art des Vorfalls** | **Kurzbeschreibung des Vorfalls** | **Zuständiges Team** | **Detaillierte Beschreibung (Auswirkung, Dauer, betroffene Aktivitäten, zugewiesene Ressourcen usw.)** | **Beschreibung der ergriffenen Maßnahmen** |
| **1** |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |
| **usw.** |  |  |  |  |  |  |

### 4.3 Schritt 3: Aktivierung und Verarbeitung

Das Hauptziel besteht darin, die Auswirkungen des Vorfalls auf die Geschäftskontinuität des Unternehmens schnellstmöglich zu verringern.

Vorfall-Tickets werden im Falle eines Vorfalls vom Vorfallreaktionsteam bearbeitet. Der Leiter des Vorfallreaktionsteams (Leader) überwacht alle Tickets. Folgende Maßnahmen müssen angesichts eines Vorfalls ergriffen werden:

| **Maßnahme** | **Befugte Funktion** | **Verbindungen zu anderen Dokumenten**  ***Name und Referenz*** |
| --- | --- | --- |
| Durchführung einer raschen Analyse der Situation auf der Grundlage der verfügbaren Informationen | Helpdesk-Mitarbeiter |  |
| Bestimmen der Maßnahmen für die Rückkehr zu einem minimal zulässigen Betriebsniveau | Leiter des Helpdesk-Teams |  |
| Eskalation des Vorfalls entsprechend seinem Schweregrad | Leiter des Helpdesk-Teams an den Leiter des Vorfallreaktionsteams |  |
| Ausführen der zu ergreifenden Maßnahmen | Incident Response Team |  |
| usw. |  | Siehe Verfahren Geschäftskontinuitätsplan und Crisis Management Plan |

### 4.4 Schritt 4: Beseitigung

Es ist nicht immer möglich, während des Vorfalls die Ursachen des Vorfalls zu ermitteln. In derartigen Fällen gilt es, sich zunächst mit den Folgen (Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs) zu befassen, bevor die Ursache ermittelt werden kann. Es müssen jedoch angemessene Anstrengungen unternommen werden, um die Ursache zu ermitteln und das Risiko eines erneuten Auftretens eines solchen Vorfalls zu begrenzen.

### 4.5 Schritt 5: Deaktivierung

Wenn die von einem Vorfall betroffenen Abteilungen zum Normalbetrieb zurückgekehrt sind, kann der Vorfall vom Vorfallreaktionsteam in Absprache mit dem Leiter des Geschäftskontinuitätsplans bzw. des Crisis Management Plan abgeschlossen werden.

Der Incident Response Plan wird deaktiviert und eine „Post Incident Review“ wird durchgeführt (siehe Schritt 6).

Folgende Maßnahmen müssen ergriffen werden:

| **Maßnahme** | **Funktion** | **Verbindungen zu anderen Dokumenten** |
| --- | --- | --- |
| Abschluss des Vorfall-Tickets | Incident Management Team | Ticket im Rahmen des Vorfallmanagements |
| Aussetzen des Incident Response Plans | Vorfallmanager |  |
| Durchführen der Post Incident Review | Incident Management Team | Post Incident Review (Dokument) |
| usw. |  |  |

### 4.6 Schritt 6: Erkenntnisse (Post Incident Review)

Ziel ist es, aus den Erfahrungen zu lernen, indem eine „Überprüfung nach dem Vorfall“ (Post Incident Review) durchgeführt wird, um das Vorfallmanagement in einem kontinuierlichen Prozess zu verbessern.

Die Überprüfung nach dem Vorfall (Post Incident Review) sollte mindestens folgende Elemente enthalten:

| **Element** | **Beschreibung** |
| --- | --- |
| **Verwaltung** |  |
| Vorfallnummer im Vorfallprotokoll: |  |
| Datum und Uhrzeit der Feststellung des Vorfalls: |  |
| Datum und Uhrzeit der Lösung des Vorfalls: |  |
| Art des Vorfalls: |  |
| Schweregrad des Vorfalls: |  |
| Waren Kunden betroffen? |  |
| Vorfallmanager: |  |
| Beschreibung des Vorfalls: |  |
| usw. |  |
|  |  |
| Feststellung |  |
| Wie und von wem wurde der Vorfall festgestellt? |  |
| Wurde der Vorfall frühzeitig erkannt oder hätte er früher erkannt werden können? |  |
| Gibt es Verfahren oder Instrumente, die zu einer frühzeitigeren Erkennung von Vorfällen eingesetzt werden können? |  |
| Wurden die Verfahren zur Meldung von Vorfällen befolgt? |  |
| usw. |  |
|  |  |
| Auswertung und Maßnahmen |  |
| Wurde der Vorfall richtig bewertet?  Waren die entsprechenden Informationen dafür verfügbar? |  |
| Welche Pläne (PMO, CMP, DRP) wurden aktiviert? |  |
| Wurde der Crisis Management Plan (CMP) aktiviert? |  |
| Welche weiteren Maßnahmen wurden zur Lösung des Vorfalls ergriffen? |  |
| Welche Ressourcen wurden zur Bewältigung des Vorfalls eingesetzt? |  |
| Ist der Plan flexibel genug, um auf unvorhergesehene Ereignisse einzugehen? |  |
| Wurden die Maßnahmen rechtzeitig ergriffen? |  |
| Welche Maßnahmen waren am nützlichsten und effektivsten? |  |
| Welche Maßnahmen wurden ergriffen, die sich als wirkungslos erwiesen haben? |  |
| Aktivitäten im Bereich der Kommunikation |  |
| Wurde (zu gegebener Zeit) eine interne Mitteilung versandt? |  |
| Wurde (zu gegebener Zeit) eine externe Mitteilung versandt? |  |
| Welche Medien wurden eingesetzt? |  |
| Wann wurde die erste Mitteilung verschickt und wie oft wurde sie aktualisiert? |  |
| Wurden die beteiligten Personen miteinbezogen? |  |
| Welche Mitteilungen sind nützlich? |  |
| Welche Mitteilungen wurden versandt, die sich als wirkungslos erwiesen haben? |  |
| Analyse der zugrunde liegenden Ursache |  |
| Wurde die Ursache des Vorfalls festgestellt? |  |
| Damit verbundene bzw. ähnliche Vorfälle? |  |
| Gibt es ein zugrunde liegendes Problem? |  |
| Wurde das zugrunde liegende Problem erkannt (siehe Schritt 4: Beseitigung) |  |
| Welche zusätzlichen Maßnahmen sind erforderlich, um etwaige zugrunde liegende Probleme zu erkennen? |  |
| usw. |  |
| Vorbeugung |  |
| Welche Erkenntnisse kann man aus den Ereignissen ziehen? |  |
| Wie kann eine Wiederholung von Vorfällen vermieden werden? Welche Maßnahmen können diesbezüglich ergriffen werden? Wer ist für die Durchführung verantwortlich? |  |
| usw. |  |
| Angemessenheit der Reaktion des Managements |  |
| Tatsächliche Zeit bis zur Wiederaufnahme (vgl. Recovery Time Objective; RTO) |  |
| Müssen die Verträge angepasst werden? |  |
| Angemessenheit der Reaktion des Managements auf den Vorfall, gemäß Business Continuity Plan: |  |
| Das Management hat nicht oder nicht zufriedenstellend reagiert. |  |
| Das Management hat reagiert, hielt sich aber nicht vollständig an die Pläne. |  |
| Das Management reagierte voll und ganz in Übereinstimmung mit den Plänen. |  |
| Grad der Vorbereitung der Mitarbeiter auf den Vorfall: |  |
| 1. Unvorbereitet |  |
| 2. Teilweise vorbereitet |  |
| 3. Vollständig vorbereitet |  |
| Folgendes könnte geändert werden, um die Wiederanlaufdauer zu verbessern: |  |
| usw. |  |

Kapitel V.  
Anhänge

## 5.1. Anhang 1. Kontaktliste

### A) Intern

| **Rolle** | **Vor- und Zuname** | **Funktion** | **Kontaktangaben**  **Geben Sie mindestens 2 Ansprechpartner pro Rolle an (1 Hauptansprechpartner und 1 Ansprechpartner im Falle von Krankheit, Urlaub, Ausscheiden des Hauptansprechpartners)** |
| --- | --- | --- | --- |
| **Teamleiter bzw. Leiter des Business Continuity Plan** |  |  | Hauptansprechpartner  @  T  M  Sonstige  @  T  M |
| **Mitglieder des Kontinuitätsmanagementteams** |  |  | Hauptansprechpartner  @  T  M  Sonstige  @  T  M |
| **Betriebsabteilung 1** |  | Grundlegende Aktivität/en (festlegen) | - Hauptansprechpartner  @  T  M  - Sonstige  @  T  M |
| **Betriebsabteilung 2** |  | Grundlegende Aktivität/en (festlegen) | - Hauptansprechpartner  @  T  M  - Sonstige  @  T  M |

### B) Extern

| **Rolle** | **Name des Unternehmens**  **Vor- und Zuname der Ansprechpartner** | **Vertragsreferenz** | **Kontaktangaben**  **Geben Sie mindestens 2 Ansprechpartner pro Rolle an (1 Hauptansprechpartner und 1 Ansprechpartner im Falle von Krankheit, Urlaub, Ausscheiden des Hauptansprechpartners)** |
| --- | --- | --- | --- |
| **Lieferant** |  |  | Hauptansprechpartner  @  T  M  Sonstige  @  T  M |
| **Lieferant** |  |  | Hauptansprechpartner  @  T  M  Sonstige  @  T  M |
| **usw.** |  |  |  |

## 5.2. Anhang 2: Referenzdokumente

* Risk Assessment & Treatment
* Business Continuity Plan
* Crisis Management Plan