Business   
Continuity Plan

Documentgeschiedenis

**GESCHIEDENIS WIJZIGINGEN**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Gewijzigd door** | **Omschrijving van de wijzigingen (V+1)** |
| **xxx** | **xxx** | **xxx** | **xxx** |
| **…** |  |  |  |

**GESCHIEDENIS GOEDKEURINGEN**

|  |  |  |
| --- | --- | --- |
| **Naam** | **Functie** | **Datum goedkeuring hoogste niveau management (directie)** |
| **xxx** | **xxx** | **xxx** |
| **…** |  |  |

Dit document geldt vanaf **[datum]**.

Dit document wordt als volgt bewaard:

1. In papieren vorm op volgende locaties: **[lijst locaties]**.
2. In digitale vorm op volgende locaties: **[locatie op bv. intranet]**.

Eigenaar van dit document is **[functie]**. Hij checkt minstens 1 maal per jaar of updates nodig zijn.

**Inhoudstafel**

[**Hoofdstuk I Doel van het document** 4](#_Toc57021120)

[**Hoofdstuk II Verbanden tussen de procedures**  5](#_Toc57021121)

[**Hoofdstuk III Kies iemand die aan het roer staat** 7](#_Toc57021122)

[3.1 Duid een beheerder voor het Business Continuity Plan aan 7](#_Toc57021123)

[3.2 Rollen van de beheerder van het Business Continuity Plan 7](#_Toc57021124)

[**Hoofdstuk IV BUSINESS CONTINUITY PLAN - BEDRIJFSCONTINUÏTEITSPLAN** 9](#_Toc57021125)

[4.1 Stap 1: Definiëren van de reikwijdte van het Business Continuity Plan: 9](#_Toc57021126)

[4.2 Stap 2: Activering van het plan 10](#_Toc57021127)

[4.3 Stap 3: Lijst de te ondernemen acties op 13](#_Toc57021128)

[4.4 Stap 4: Deactivering van het Business Continuity Plan 17](#_Toc57021129)

[4.5 Stap 5: Test uw plan en hou het up-to-date 18](#_Toc57021130)

[**Hoofdstuk V Bijlagen** 19](#_Toc57021131)

[5.1 Bijlage 1: Contactenlijst 19](#_Toc57021132)

[A) Intern 19](#_Toc57021133)

[B) Extern 21](#_Toc57021134)

[5.2 Bijlage 2: Referentiedocumenten 21](#_Toc57021135)

# Hoofdstuk I Doel van het document

**Het voornaamste doel** van een Business Continuity Plan (BCP) is de continuïteit verzekeren van de (voornaamste) activiteiten van het bedrijf in geval van een incident, crisis of ramp.

**Hoe?** Het betreft:

1. **Anticiperen** op en een coherente aanpak hanteren voor de uitvoering van een Business Continuity Plan om de belangrijkste processen in kaart te brengen en de risico's waaraan zij worden blootgesteld te analyseren;
2. **Ontwikkelen van de juiste procedures** om te weten hoe te reageren op een incident, crisis of ramp.
3. **Identificeren van de noodzakelijke elementen** (uitrusting, gebouw, mensen, zowel intern als extern, ....) om effectief procedures te implementeren die door het hoogste niveau van het bedrijfsmanagement zijn gevalideerd om incidenten, crises en rampen te beheren.

**Resultaat?**

1. **Beschikken over gevalideerde procedures**
2. **Weten hoe de impact van deze incidenten kan worden beperkt** tot een voor het bedrijf aanvaardbaar niveau.
3. **Vastleggen van objectieven en tijdspannes** om de continuïteit van de (belangrijkste) activiteiten van het bedrijf te waarborgen.

OPGELET: zelfs als de procedures zijn gevalideerd, **vergeet dan niet om regelmatig verslag uit te brengen aan het management** in het geval er zich een incident voordoet dat een impact heeft op de continuïteit van de activiteiten van het bedrijf.

**Bedreigingen**: Continuïteitsbeheer is breder dan mogelijke IT-incidenten. Overstromingen of branden, de afwezigheid van werknemers (ziekte, ontslag, overlijden), het verdwijnen van één of meerdere leveranciers die essentieel zijn voor het bedrijf, pandemie,... kunnen ook een bedreiging vormen voor de continuïteit van de activiteiten van het bedrijf. Bij de organisatie van het continuïteitsbeheer, en meer in het bijzonder bij de Risk Assessment, is het de bedoeling om alle soorten bedreigingen te identificeren die de activiteiten van het bedrijf kunnen bedreigen, waarbij ook rekening wordt gehouden met het " worst case scenario".

*Wat de identificatie van bedreigingen, kwetsbaarheden en de impact betreft: zie uw Risk Assesment en uw Risk Treatment.*

# Hoofdstuk II Verbanden tussen de procedures

Het schema (zie hieronder) laat zien hoe het “Business Continuity Plan” zich integreert met andere procedures.

Om te beschikken over een effectief Business Continuity Plan, moet u de templates voor Risk Assessment en Risk Treatment hebben ingevuld. De mate van risico en waarschijnlijkheid van een incident is afhankelijk van de Risk Treatment die u heeft uitgevoerd. Ook het beheer van een incident zal sterk afhangen van de preventieve en herstellende maatregelen die u hebt genomen.

**A**

Bij het opstellen van uw Business Continuity Plan en uw incidentenbeheerplan, kan het nodig zijn om uw Risk Assessment te updaten (vooral omdat u van plan bent om de risico's aan te passen door nieuwe tools aan te schaffen of nieuwe projecten te lanceren).

**B**

Uw Risk Assessment en Business Continuity Plan vereist ook dat u navraag doet bij uw leveranciers, uw contracten herziet en zelfs bepaalde Service Level Agreements (SLA's) of clausules oplegt aan uw leveranciers.

**C**

De continuïteit van activiteiten is nauw verbonden met het beheren van incidenten, omdat u ervoor moet zorgen dat u ook in het geval van een incident de activiteiten (minimum de essentiële) van het bedrijf kunt voortzetten. De beheerder van het Business Continuity Plan stuurt de benodigde informatie door naar de beheerder van het incidentenbeheerplan om incidenten te beheren.

**D**

**E**

In het bijzonder kunt u zich via uw klanten of leveranciers bewust worden van een lopend incident.

De meeste incidenten houden niet noodzakelijkerwijs de activering van het Business Continuity Plan in, simpelweg omdat het "gewone" kleine incidenten zijn die geen echte impact hebben op het bedrijf. Als er een incident met een bedrijfsimpact plaatsvindt, meldt beheerder van het incidentenbeheerplan dit aan de beheerder van het Business Continuity Plan die het Business Continuity Plan activeert. Tijdens het incident zorgt de beheerder van het incidentenbeheerplan voor een regelmatige rapportage aan de beheerder Business Continuity Plan. Na het incident stuurt de beheerder van het incidentenbeheerplan de "Post incident review" door naar de beheerder van het Business Continuity Plan.

**F**

Als het incident geen invloed heeft op de continuïteit van de activiteiten, kan de beheerder van het incidentenbeheerplan, indien nodig, klanten en leveranciers waarschuwen dat het bedrijf een klein incident meemaakt.

**G**

Indien het incident impact heeft op de bedrijfscontinuïteit, zal de beheerder van het Business Continuity Plan, indien nodig, klanten en leveranciers aanspreken op basis van de informatie die door de functionele diensten en de beheerder van het incidentenbeheerplan wordt verstrekt.

**H**

Na een incident kan de post-incident review aangeven dat de Risk Assessment en de Risk Treatment moeten worden aangepast.

**I**

Na een incident kan de post-incident review aangeven dat u de contracten met uw leveranciers moet herzien.

**J**

Na het beheren van incidenten is het mogelijk dat u uw Risk Assessment en Risk Treatment moet herzien of dat uw Business Continuity Plan moet worden verbeterd. **Voor meer informatie over de verschillende procedures, zie de meegeleverde templates**.

Om het uitgewerkte plan in geval van een incident effectief te laten werken, is het belangrijk dat de geplande **procedures** **vooraf grondig worden getest en regelmatig worden herzien**. Denk eraan om ten minste één keer per jaar en na elke gebeurtenis/crisis of ramp uw plannen te herzien en "geleerde lessen" te identificeren, zodat u de plannen kunt verbeteren op basis van de behoeften en de ervaring van het bedrijf.

Iedereen die betrokken is bij het Business Continuity Plan moet zijn exacte rol kennen en de meest recente versie van het plan hebben. (Vergeet niet om ook een papieren versie van het plan te bewaren).

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**3. Incidentenbeheerplan**

**Essentiële leveranciers**

**Klanten**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

# Hoofdstuk III Kies iemand die aan het roer staat

## 3.1 Duid een beheerder voor het Business Continuity Plan aan

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

*Murphy’s Law*

Het incident kan zich voordoen op een vrijdagavond, een weekend, de dag voor een groot contract of tijdens de feestdagen,...

Het is daarom beter om op voorhand na te denken over mogelijke incidenten dan volledig onvoorbereid te zijn op het moment dat het incident zich daadwerkelijk voordoet...

Denk er dus aan om iemand aan te duiden die "aan het roer zal staan", alsook een andere persoon die deze persoon kan vervangen in geval van afwezigheid/vertrek/ziekte.

*Wie kiezen*? Idealiter zou deze persoon een goede communicator moeten zijn, het bedrijf goed genoeg kennen, stressbestendig zijn en voldoende ervaring hebben. In grotere organisaties kan een "team" worden aangesteld.

Dit kan het management zijn of iemand met de bevoegdheid om een strategische-operationele rol op zich te nemen.

Opgelet: “beheerder” betekent niet altijd "verantwoordelijke", de beheerder moet mogelijk op meerdere interne verantwoordelijken een beroep doen, maar het is vanzelfsprekend dat belangrijke beslissingen en de eindverantwoordelijkheid bij het hoogste niveau van het management liggen. Daarom is het belangrijk dat alle procedures door het management worden gevalideerd.

## 3.2 Rollen van de beheerder van het Business Continuity Plan

De beheerder van het Business Continuity Plan moet ervoor zorgen dat er binnen het bedrijf een constructieve dialoog wordt gevoerd, de samenwerking tussen de betrokken afdelingen of personen bevorderen en zorgen voor de rapportage aan het management.

De beheerder van het Business Continuity Plan (of het nu gaat om een individu of een teamleider, afhankelijk van de grootte en de behoeften van het bedrijf):

1. Stelt het Business Continuity Team samen (als dat er is) en neem contact op met de sleuteldeskundige(n) (IT-diensten, veiligheids- en preventieadviseur, functionaris voor gegevensbescherming (DPO), informatieveiligheidsadviseur....);
2. Houdt een eerste bijeenkomst (met het Business Continuity Team als dat er is en bij gebrek daaraan met het management) om de impact van het incident te beoordelen en de mate van kriticiteit van het incident en de gïmpacteerde activiteiten te bepalen. (Het is mogelijk om de situatie opnieuw te evalueren afhankelijk van de omstandigheden. Het betreft hier slechts een eerste beoordeling);
3. Informeert en rapporteert aan het management op een regelmatige basis;
4. Activeert het Business Continuity Plan;
5. Identificeert, indien mogelijk, hoe het incident zich zou kunnen ontwikkelen. Bepaal welke informatie nog ontbreekt om de situatie beter te begrijpen en hoe deze informatie binnen een bepaald tijdsbestek zal worden verzameld (opgelet: het gaat niet om het verzamelen van *alle* informatie in dit stadium, maar alleen de meest urgente informatie, d.w.z. datgene wat nodig is voor een eerste beoordeling van het huidige en waarschijnlijke niveau van kriticiteit van het incident);
6. Neemt, indien nodig, contact op met de communicatiediensten en de klantenrelatiediensten (indien aanwezig) of stelt, indien nodig, het management een communicatieplan voor t.a.v. de klanten en leveranciers (zie de fiche "Communicatie");
7. Neemt contact op met de betrokken functionele verantwoordelijken en geeft hun de in dit stadium verzamelde informatie door;
8. Onderhoudt een dialoog met de betrokken functionele diensten en zorgt voor rapportage op managementniveau gedurende het gehele incident;
9. Kan de vermindering of onderbreking van een niet-essentiële activiteit bevelen om over de nodige middelen voor de essentiële activiteiten te beschikken ;
10. Kan zorgen voor de evacuatie van medewerkers en klanten;
11. Kan communiceren met klanten en leveranciers (externe communicatie);
12. Beëindigt de activering van het Business Continuity Plan;
13. Neemt deel aan het “post incident review” na afloop van het incident;
14. Zorgt voor de herziening van de plannen (eventuele wijzigingen volgens de behoeften en de opgedane ervaring) en de validering van de plannen door het management;
15. Organiseert de nodige oefeningen en tests om de bewustwording te vergroten en het Business Continuity Plan bij te werken;
16. Houdt de plannen beschikbaar voor sleutelpersonen (ook op papier en buiten een eventuele overstromingszone);
17. *… [identificeer eventuele andere rollen]*

NB: In sommige organisaties is het mogelijk:

* dat één persoon of team het beheer van alle incidenten overneemt.
* dat buitenstaanders betrokken zijn bij het proces. Bijvoorbeeld een advocatenkantoor, externe gegevensbeschermingsfunctionarissen, verzekeraars,…
* dat bepaalde stappen niet plaatsvinden (zoals bijvoorbeeld stap 6 en 7).

# Hoofdstuk IVBUSINESS CONTINUITY PLAN - BEDRIJFSCONTINUÏTEITSPLAN

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

*General Dwight D. Eisenhower*

Het is onmogelijk om alles te voorzien, plotselinge en onvoorspelbare gebeurtenissen kunnen zich altijd voordoen.

Wanneer een incident zich voordoet, heeft uw plan misschien niet "aan alles gedacht", maar het simpele feit dat u zich heeft voorbereid op andere soorten incidenten en bent gaan nadenken over de bedrijfscontinuïteit zal u helpen om veerkrachtiger te zijn en in staat te zijn om op zijn minst de essentiële activiteiten van uw bedrijf te blijven uitvoeren.

Een bedrijfscontinuïteitsplan is gebaseerd op 5 stappen:

Stap 1: Definiëren van de reikwijdte van het Business Continuity Plan

Stap 2: Activeren van het plan

Stap 3: Deactivering van het plan

Stap 4: Test en houd uw plan up-to-date

## 4.1 Stap 1: Toepassingsgebied van het Business Continuity Plan:

Een Business Continuity Plan is een iteratief (herhalend) proces:

Voor een eerste iteratie, focus op de essentie: welke activiteiten zijn essentieel voor het economisch overleven van uw bedrijf? Hou in het bijzonder rekening met:

* hoeveel van de omzet deze activiteiten genereren;
* het aantal klanten voor deze activiteit;
* de impact indien de activiteit moet worden teruggeschroefd of stilgelegd: impact op de productiviteit, de financiën en/of de reputatie van het bedrijf.

Misschien wilt u uw Business Continuity Plan in eerste instantie beperken tot deze kritische activiteiten.

NB: Uw Risk Assessment zou u reeds moeten geholpen hebben om de zaken duidelijker te zien in dit stadium.

| Essentiële activiteit 1 |
| --- |
| Lijst van essentiële elementen om de continuïteit van de betrokken essentiële bedrijfsactiviteit te kunnen verzekeren |
| Sleutelpersoneel |
| Belangrijke informatie of gegevens |
| Noodzakelijke IT-diensten (hardware, software) |
| Gebouwen |
| … |

## 4.2 Stap 2: Activering van het plan

De beheerder van het Business Continuity Plan kan het plan activeren, bijvoorbeeld omdat de overheid of de regulator van de sector ordemaatregelen heeft genomen, omdat leveranciers hebben aangegeven dat er een tekort is aan een essentieel element, of omdat de beheerder van het incidentenbeheerplan heeft gewaarschuwd dat er een impact kan zijn op de continuïteit van de activiteiten van het bedrijf.

|  |
| --- |
| **SAFETY FIRST: Bescherm het menselijk leven eerst!** |

Het spreekt voor zich, maar nog voordat de continuïteit van de activiteiten van het bedrijf gewaarborgd kan worden, gaat het er eerst om menselijk levens te beschermen. Dit houdt ook in dat er, afhankelijk van de omstandigheden van het bedrijf, passende maatregelen moeten worden genomen.

Bijzondere aandacht moet worden besteed aan de risico's van brand, explosie, blootstelling aan giftige producten, overstroming,…

De beheerder of het team dat verantwoordelijk is voor het Business Continuity Plan voert de volgende controles en/of acties uit om het welzijn van de mensen te verzekeren:

1. Identificatie van incidentscenario's
2. Identificatie van de soorten risico's
3. Preventieve maatregelen
4. Beheersmaatregelen
5. Onderzoek van het incident na afloop.

Deze regeling is identiek aan het incidentenbeheerplan waarvan de beheerder van het Business Continuity Plan ook op de hoogte moet zijn.

**Voorbeeld**

**Scenario:** Gevaarlijke producten vloeien weg of verdampen abnormaal, gewapende personen betreden gebouwen, er woedt een epidemie of pandemie in de regio waar de werkplekken zich bevinden of in de omgeving, het drinkwater is besmet, een brand of overstroming bedreigt de gebruikelijke werkplekken (brand in een nabijgelegen gebouw, nabijheid van reeds overstroomde en door overstromingen bedreigde gebieden),…

**Risico’s**: In gevaar brengen van het personeel, verwondingen, sterfgevallen en psychologische gevolgen moeten in overweging worden genomen.

**Preventieve maatregelen:**

* Identificeer het verplichte wettelijke kader (Code van welzijn op het werk,...) en raadpleeg de website van de [FOD Werkgelegenheid](https://werk.belgie.be/nl/themas/welzijn-op-het-werk), de website van het [European Agency for Safety and Health at work](https://oiraproject.eu/en/oira-tools) en het Belgisch Kenniscentrum over Welzijn op het Werk ([BeSWIC](https://www.beswic.be/nl)).
* Voldoen aan wettelijke en/of reglementaire verplichtingen (brandmelders, branddeuren,...).
* Identificeer de onmisbare deskundigen en definieer de rollen en verantwoordelijkheden vóór elk incident.
* Identificeer de noodnummers en de middelen om contact met hen op te nemen.
* Zorg voor een defibrillator in het gebouw
* Maak het personeel bewust van goede praktijken (niet roken op het terrein, geen deuren of ramen open laten staan, elk incident dat anderen in gevaar zou kunnen brengen onmiddellijk melden, personeel opleiden in elementaire eerste hulp, etc.).
* Zorg voor evacuatieplannen (brand, overstroming, enz.) en test deze regelmatig (minstens één keer per jaar).
* Identificeer mensen die meer risico lopen (moeilijkheden om zich te verplaatsen, te ademen,...) of die bijzonder gevoelig zijn (hart, ademhalingsmoeilijkheden,...).

**Beheersmaatregelen**

Afhankelijk van het niveau van kriticiteit van het incident wordt het incident eerst gekwalificeerd door de beheerder van het incidentenbeheerplan. Als er een risico bestaat dat de activiteiten van het bedrijf worden beïnvloed, stelt de beheerder van het incidentenbeheerplan de beheerder van het Business Continuity Plan op de hoogte. (NB: in kleinere structuren is het mogelijk dat één en dezelfde persoon deze verschillende functies op zich neemt).

Deze eerste evaluatie gebeurt snel en moet mogelijk in de loop van een incident worden herzien.

|  | Actie | Wie doet wat? | Verwijzingen naar andere documenten |
| --- | --- | --- | --- |
|  | Beschrijving van de actie | Functies en rollen van de sleutelpersonen die belast zijn met de uitvoering van de actie | Referentie naar andere documenten |
|  | Kennisname van de wettelijke verplichtingen met betrekking tot de preventie van beroepsrisico's en de bescherming van de veiligheid en gezondheid op het werk. |  |  |
|  | Raadpleeg de website van BESWIC  <https://www.beswic.be/nl>  Checklists zijn beschikbaar bij de FOD Werkgelegenheid volgens het type gevreesde gebeurtenis (pandemie,...).  Er zijn ook instrumenten beschikbaar bij het European Agency for Safety and Health at Work  <https://oiraproject.eu/en/oira-tools> |  |  |
|  | Beschikken over adequate procedures (incidentenbeheer) |  |  |
|  | Definiëren van rollen en verantwoordelijkheden (voorafgaand aan een incident) |  |  |
|  | Identificeren van alle beheersmaatregelen (zie incidentmanagement) |  |  |
|  | Identificeren en bijhouden van een lijst van hulpdiensten en interne en externe contactpersonen. |  |  |
|  | Informeren van medewerkers en eventueel externe stakeholders (klanten, leveranciers) dat er een incident plaatsvindt en dat er maatregelen worden genomen om dit aan te pakken. |  |  |
|  | Bijhouden van incidentlogboeken (logs, bewijsmateriaal, sporen |  |  |
|  | Overwegen om regelmatig contact op te nemen met de (families van) mogelijke gewonden. |  |  |
|  | … |  |  |

## 4.3 Stap 3: Lijst de te ondernemen acties op

Vergeet uw Risk Assessment en Risk Treatment niet: u heeft al vele stappen ondernomen om het risico te verminderen of de impact van een incident te beperken. Als u andere acties overweegt bij het ontwikkelen van uw Business Continuity Plan, vergeet dan niet om uw Risk Assessment en uw Risk Treatment up-to-date te houden. Het Business Continuity Plan is ook gekoppeld aan het Incidentenbeheerplan (zie template Incidentenbeheer).

De beheerder of het team van het Business Continuity Plan neemt de nodige stappen om de schade die door het incident wordt veroorzaakt te beperken en te minimaliseren en om essentiële activiteiten te behouden. Een van de dingen die u kunt doen bij het schrijven van uw Business Continuity Plan is het ontwikkelen van checklists. Merk echter op dat het onmogelijk is om alle incidentscenario's te identificeren en dat het veel belangrijker is dat het team zich kan aanpassen aan de omstandigheden. Zodra het betrokken personeel op de hoogte is van deze plannen, zal het bedrijf beter in staat zijn om te reageren op elk incident dat zich kan voordoen.

*Vul deze tabel in volgens de situatie van uw bedrijf:*

| **Actie** | **Wie doet wat?** | **Verwijzingen naar andere documenten** |  |
| --- | --- | --- | --- |
| Beschrijving van de actie | Functies en rollen van de sleutelpersonen die belast zijn met de uitvoering van de actie | Referentie naar andere documenten | Ok? |
| Identificeren van belangrijke processen en activiteiten die worden verstoord en beschrijven van de impact op de dienstverlening. |  |  |  |
| identificeren van de (risico's op) schade, zowel materieel als immaterieel (bv. reputatie). |  |  |  |
| Acties vaststellen om ervoor te zorgen dat de situatie niet verslechtert.   * Laat deze keuzes valideren door het management |  |  |  |
| Identificeren wat intact is ("wat nog werkt") |  |  |  |
| Acties om extra middelen in te zetten, zowel via eigen personeel als via onderaannemers.   * Laat deze keuzes valideren door het management |  |  |  |
| … |  |  |  |

#### Scenario: Het hoofdgebouw is niet toegankelijk

| Element  (beschrijving) | Schade  (beschrijving) | Acties en instructies | Geschatte hersteltijd |
| --- | --- | --- | --- |
| Bv. Nationale staking die de toegang tot uw hoofdgebouw blokkeert.  Bv. Stroomonderbreking of afschakeling van elektriciteit die de toegang onmogelijk of moeilijk maakt. | Identificeren van de belangrijke processen en activiteiten die worden verstoord en het beschrijven van de impact op de dienstverlening.  Identificeren van de (risico's op) schade, zowel materiële als immateriële (bv. reputatie).  Identificeren wat intact is ("wat nog werkt") | Opstellen van een lijst met preventieve maatregelen *(verband met de Risk Treatment en het Incidentenbeheerplan)*  Opstellen van de lijst met beheersmaatregelen  *Acties vaststellen om ervoor te zorgen dat de situatie niet verder verslechtert.*  *Acties identificeren om extra middelen in te zetten, zowel via eigen personeel als via onderaannemers.*  Bv. zet werknemers op telewerk (voor degenen die niet staken), waarschuwt leveranciers om niet op het gebruikelijke adres te leveren, waarschuwt klanten om niet naar het hoofdgebouw te gaan en specificeert de mogelijke gevolgen voor de levertijden.  Bv. neem contact op met de elektricien of de beheerder van het elektriciteitsnet(zie ook de bovenstaande maatregelen). | Bv. 1 dag, 1 week  Bv. 4 uren of 1 week,… |
| … |  |  |  |

#### Scenario: Onderbreking van de verbinding met de cloud of het datacenter

| Element  (beschrijving) | Schade  (beschrijving) | Acties en instructies | Geschatte hersteltijd |
| --- | --- | --- | --- |
| Uw bedrijf heeft geen toegang meer tot gegevens en bestanden die niet lokaal zijn opgeslagen.. | Identificeren van de essentiële activiteiten (zie stap 1) die worden geïmpacteerd en het beschrijven van de impact op deze activiteiten. | Opstellen van een lijst met preventieve maatregelen *(verband met de Risk Treatment en het Incidentenbheerplan)*  Bv. minimum een lokale kopie bewaren,...  Opstellen van de lijst met beheersmaatregelen  Acties vaststellen om ervoor te zorgen dat de situatie niet verslechtert.  *Acties vaststellen om ervoor te zorgen dat de situatie niet verder verslechtert.*  *Acties identificeren om extra middelen in te zetten, zowel via eigen personeel als via onderaannemers.*  Bv. neem contact op met de cloud provider of de datacentermanager en bepaal de geschatte hersteltijd, vraag om realtime op de hoogte te worden gehouden.  Bv. de contractuele boetes toepassen voor het niet respecteren van het overeengekomen niveau van dienstverlening (SLA). | Bv. 5u tot 2 dagen |

#### Scenario: Overstroming

| Element  (beschrijving) | Schade  (beschrijving) | Acties en instructies | Geschatte hersteltijd |
| --- | --- | --- | --- |
| Een overstroming | Identificeren van de essentiële activiteiten (zie stap 1) die worden geïmpacteerd en het beschrijven van de impact op deze activiteiten. | Opstellen van een lijst met preventieve maatregelen *(verband met de Risk Treatment en het Incidentenbeheerplan)*  ZIE FICHE OVERSTROMING  Opstellen van de lijst met beheersmaatregelen  *Acties vaststellen om ervoor te zorgen dat de situatie niet verder verslechtert.*  *Acties identificeren om extra middelen in te zetten, zowel via eigen personeel als via onderaannemers.*  Bv.: telewerken voor werknemers, contact opnemen met verzekeraars, manuele of pneumatische afvoer van modderig water, ... | Bv. 1 week |

#### Scenario: …

| Element  (beschrijving) | Schade  (beschrijving) | Acties en instructies | Geschatte hersteltijd |
| --- | --- | --- | --- |
| ..... |  | ... | .... |

## 4.4 Stap 4: Deactivering van het Business Continuity Plan

De deactivering van het Business Continuity Plan wordt uitgevoerd door de beheerder van het Business Continuity Plan, in overleg met het management.

Het Business Continuity Plan kan m.n. worden gedeactiveerd, wanneer het incident wordt afgesloten of wanneer er geen/geen verdere impact is op de essentiële activiteiten van het bedrijf (zelfs als het incident nog loopt, bijvoorbeeld omdat er een tijdelijke oplossing is gevonden).

| **Criteria voor de deactivering van het Business Continuity Plan** |
| --- |
| Zijn alle niveaus van dienstverlening teruggekeerd naar het normale niveau of op het minimaal aanvaardbare niveau? |
| Is er enige reden om te betwijfelen of het niveau van de dienstverlening de komende dagen op een stabiele manier zal worden bereikt? |
| Zijn de beheersmaatregelen (inclusief tijdelijke oplossingen) gedeactiveerd? |
| Zijn de operationele teams (functionele diensten) voldoende uitgerust om mogelijke gevolgen na een incident op te vangen? |
| Heeft de uiteindelijke communicatie met externe partijen (klanten, leveranciers,...) plaatsgevonden? |
| ... |

In het kader van de deactivering van het Business Continuity Plan moeten de gebeurtenissen worden beschreven, zodat de volgende activering van het plan kan worden verbeterd.

| **Actie** | **Wie doet wat?** | **Verwijzingen naar andere documenten** |
| --- | --- | --- |
| Korte beschrijving van de ondernomen acties (beheersmaatregelen) |  |  |
| Verwijs naar de Post Incident Review |  |  |
| Neem contact op met de verzekeraars |  |  |
| Zet een ‘einde incident/crisis’-communicatie op ter attentie van de betrokken externe personen (klanten, leveranciers). |  |  |
| Vaststellen of er gebieden van het Business Continuity Plan zijn die voor verbetering vatbaar zijn (met inbegrip van de externe contractuele betrekkingen). |  |  |
| Toepassing van mogelijke contractuele sancties wanneer niet aan de dienstverleningsniveaus (SLA's) is voldaan. |  |  |

**Het Post incident Review**

Het is nu een kwestie van het toevoegen van het Post incident review aan het Business Continuity Plan deactiveringsrapport. (Zie Incidentenbeheerplan en de fiches).

## 4.5 Stap 5: Test uw plan en hou het up-to-date

***“*** ***Een plan dat op een plank slaapt, is het papier waarop het is gedrukt niet waard”***

Immers, als het Business Continuity Plan stoffig wordt, is de kans groot dat in het geval van een incident niemand weet hoe het moet worden toegepast. Regelmatige sensibilisering is noodzakelijk.

Denk eraan het personeel op te leiden en denk na over de verschillende communicatiekanalen (posters, bewegwijzering, oefeningen, hulpmiddelen). Voor ideeën over tools zie : [BeSWIC](https://www.beswic.be/nl/in-de-praktijk/veiligheidsinstructietool-toworksafe-om-anderstalige-werknemers-veilig-te-laten-werken) over veiligheid van werknemers; [Cyber Security Coalition](https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/) over cybersecurity; [FOD Werkgelegenheid](https://werk.belgie.be/nl/nieuws/coronavirus-sensibiliseringsmateriaal-voor-op-de-werkplek-17-talen) over pandemieën;...

|  |  |  |
| --- | --- | --- |
| **Maatregelen** | **Opmerkingen** | **Ok ?** |
| Aanwijzing van een beheerder plus een back-up in geval van afwezigheid van de beheerder  of  Een team aanwijzen dat zal instaan voor het Business Continuity Plan (plus een leader) |  |  |
| Zorg ervoor dat het personeel ten minste eenmaal per jaar wordt opgeleid en wanneer er belangrijke updates worden doorgevoerd. |  |  |
| Regelmatig een oefening organiseren (min. één keer per jaar) |  |  |
| Zorg voor de nodige contacten (leveranciers, advocaten, verzekeraars, enz.) en controleer of de contacten up-to-date zijn (minstens één keer per jaar). |  |  |
| Test de procedures voor back-up en herstel van gegevens regelmatig (idealiter per kwartaal). |  |  |
| Update het Business Continuity Plan volgens de mensen (aankomst/vertrek) en omstandigheden (nieuwe projecten, nieuw beheer van interne procedures, enz.). |  |  |

# Hoofdstuk V Bijlagen

## 5.1 Bijlage 1: Contactenlijst

### A) Intern

#### Deskundigen

| Rol | Voornaam en NAAM | Functie | Contact  Vergeet niet om minstens 2 contacten per rol te hebben (1 hoofdcontact en 1 in geval van ziekte, verlof, vertrek van het hoofdcontact) |
| --- | --- | --- | --- |
| Leider van het Business Continuity Team of beheerder van het Business Continuity Plan |  |  | Hoofdcontact  @  T  M  Andere  @  T  M |
| Leden van het Business Continuity Plan-team |  |  | Hoofdcontact  @  T  M  Andere  @  T  M |
| Functionele dienst 1 |  | Essentiële activiteiten (identificeer) | Hoofdcontact  @  T  M  Andere  @  T  M |
| Functionele dienst 2 |  | Essentiële activiteiten (identificeer) | Hoofdcontact  @  T  M  Andere  @  T  M |
| … |  |  |  |

### B) Extern

#### Leveranciers, klanten,…

| Rol | Naam van de onderneming  Voornaam en NAAM van de contactpersonen | Referentie naar contract(en) | Contact  Vergeet niet om minstens 2 contacten per rol te hebben (1 hoofdcontact en 1 in geval van ziekte, verlof, vertrek van het hoofdcontact) |
| --- | --- | --- | --- |
| Leverancier 1 |  |  | Hoofdcontact  @  T  M  Andere  @  T  M |
| Klant 1 |  |  | Hoofdcontact  @  T  M  Andere  @  T  M |
| ... |  |  |  |

## 5.2 Bijlage 2: Referentiedocumenten

1. Risk Assessment en Risk Treatment
2. Incidentenbeheerplan
3. Crisis Management Plan
4. …