

CRISISCOMMUNICATIE

 In samenwerking met:



# Crisiscommunicatie

Elk bedrijf wordt geconfronteerd met crisissen. De oorzaak van veel van deze crisissen ligt buiten de organisatie. Vaak dwingen onvoorziene omstandigheden waar u geen vat op hebt uw bedrijf om onmiddellijk te reageren.

Als een crisis toeslaat, ontstaat er snel en gemakkelijk paniek. Dat kunt u voorkomen door vast te houden aan uw crisisplan. Dat beschrijft hoe u met de situatie kunt omgaan. Voor de reputatie van uw organisatie is de manier waarop u de crisis aanpakt, doorslaggevend, niet de crisis zelf.

**Disclaimer**

De informatie in dit document is bedoeld om de werkgever stof tot nadenken te geven in het kader van incidentenbeheer om de bedrijfscontinuïteit te verzekeren. Het is dus niet de bedoeling om autoriteiten die verantwoordelijk zijn voor het toezicht op de veiligheid op het werk te vervangen. Deze informatie ontslaat de werkgever niet van de verplichting om zich te houden aan de reglementaire bepalingen die van toepassing kunnen zijn op elke specifieke werksituatie.

Dit betekent dat het gebruik van dit document door de werkgever altijd afhankelijk is van zijn pragmatisch oordeel en dat het aan hem is om de elementen en omstandigheden te beoordelen, zowel in feite als in rechte, waarmee de werkgever in welomschreven en concrete gevallen op de werkplek te maken krijgt.

*Voor meer informatie over de verschillende stappen, zie het “Incidentenbeheerplan”, hoofdstuk III.*

*.*

**CRISISCOMMUNICATIE**

[I. Stap 1: Voorbereiding (VOOR HET INCIDENT) 4](#_Toc57830017)

[1.1: Kies iemand die aan het roer staat 4](#_Toc57830018)

[1.2: Ken uw risico’s 4](#_Toc57830019)

[1.3: Preventieve maatregelen 5](#_Toc57830020)

[II. Stap 2: Melding en identificatie 10](#_Toc57830021)

[2.1: Melding 10](#_Toc57830022)

[2.2: Identificatie 10](#_Toc57830023)

[III. Stap 3: Activering en behandeling (INCIDENT) 12](#_Toc57830024)

[3.1: Identificeer uw instrumenten en middelen 12](#_Toc57830025)

[3.2: **BEHEERSMAATREGELEN** 14](#_Toc57830026)

[IV. Stap 4: Eradication 15](#_Toc57830029)

[V. Stap 5: Deactivering 15](#_Toc57830030)

[VI. Stap 6: Geleerde lessen (post incident review) (NA HET INCIDENT) 16](#_Toc57830031)

[6.1: Context: verzamel de juiste informatie 16](#_Toc57830032)

[6.2: Evaluatie van het incident en geleerde lessen 16](#_Toc57830033)

[VII. Bijlagen 20](#_Toc57830034)

[7.1: Contactenlijst 20](#_Toc57830035)

[7.2: Tabel 22](#_Toc57830036)

## Stap 1: Voorbereiding (VOOR HET INCIDENT)

Zie Risk Assessment et Risk Treatment.

### 1.1: Kies iemand die aan het roer staat

|  |
| --- |
| **Wie kan dit incidentenbeheerplan opstellen ?**  **Wie kan dit plan valideren (management)?** |

*Zie Bijlage VII, 7.2: Tabel*

In grote bedrijven kan een groep (idealiter multidisciplinair en inclusief) worden gevormd.

In kleinere bedrijven kan één en dezelfde persoon door het management worden aangesteld of kan het management zelf deze rol op zich nemen. In dit geval is het echter raadzaam om een back-up aan te wijzen (een persoon die hem/haar kan vervangen in geval van afwezigheid, ziekte of vertrek).

Zorg ervoor dat u de procedures/het incidentenbeheerplan laat valideren, alsook het huidige document.

### 1.2: Ken uw risico’s

|  |
| --- |
| **Heeft u een Risk Assessment gerealiseerd ?**  **Heeft u een Risk Treatment gerealiseerd ?** |

*Zie Bijlage VII, 7.2: Tabel*

Opdat het incidentenbeheerplan effectief zou zin, moet het bedrijf zijn risico’s geïdentificeerd, geanalyseerd en geëvalueerd hebben. Dat is het doel van een Risk Assessment (zie template). Het is ook noodzakelijk dat de maatregelen om die risico’s te behandelen, gekend zijn. at is het doek van een Risk Treatment (zie template).

Verschillende scenario's dienen onderzocht te worden.

Er kan een onderscheid gemaakt worden tussen **drie soorten crisissen**, naargelang de oorzaken ervan en hoe deze de reputatie van de organisatie beïnvloeden. Belangrijk om te weten is dat de bedreiging voor de reputatie van de organisatie vaak afhangt van eerdere crisissen en het reeds bestaande imago van de organisatie in kwestie.

**Scenario’s:**

1. **Slachtoffercrisis**

Een slachtoffercrisis doet zich voor wanneer de organisatie wordt gezien als slachtoffer van de crisis. Een vaak voorkomend voorbeeld is een natuurramp. Als een brand bijvoorbeeld de fysieke infrastructuur van een bedrijf vernietigt, kan het bedrijf geen zaken meer doen. In dit geval wordt de reputatie van de organisatie niet of nauwelijks aangetast, omdat de situatie onvermijdelijk is en het bedrijf deze niet kan voorkomen.

1. **Accidentele crisis**

Bij een accidentele crisis heeft de organisatie schuld aan de crisis, maar waren haar acties onbedoeld. Zelfs wanneer dit soort crisis triviaal lijkt, is het belangrijk om deze crisis snel aan te pakken voordat ze tijd heeft om te escaleren.

1. **Te voorkomen crisis**

Wanneer de organisatie een berekend risico neemt dat tot een negatieve uitkomst of gebeurtenis leidt, spreken we over een “te voorkomen crisis”. Dat soort crisis houdt een grote bedreiging in voor een organisatie, omdat de reputatie op het spel staat. In dergelijke situatie zijn de reacties en acties van de organisatie op de crisis cruciaal. Ondanks die maatregelen is het na zo’n crisis buitengewoon moeilijk om uw merkreputatie weer op te bouwen.

### 1.3: Preventieve maatregelen

Op de drie bovenstaande scenario’s zijn er verschillende **responsstrategieën** mogelijk die organisaties kunnen gebruiken om een ​​incident/crisis het hoofd te bieden. Het vertrekt vanuit wie verantwoordelijk was voor het veroorzaken van de crisis en hoe groot de bedreiging is voor de reputatie van het bedrijf.

Meer bepaald zijn er vier belangrijke communicatiestrategieën:

1. **Heropbouwstrategie**

Deze strategie heeft tot doel de relaties met belanghebbenden weer op te bouwen door de reputatie van de organisatie te herstellen. Dit wordt bereikt door verantwoordelijkheid te nemen voor de crisis en excuses te bieden aan degenen die door de uitkomst worden getroffen.

1. **Inperkstrategie**

Deze strategie werkt door de hoeveelheid verantwoordelijkheid die op de organisatie wordt gelegd te minimaliseren. Dit wordt bereikt door excuses aan te bieden of door de acties van het bedrijf te rechtvaardigen.

1. **Ontkenstrategie**

Deze strategie neemt de schuld volledig weg bij de organisatie. Dit wordt bereikt door de “aanklager(s)” te confronteren met hun ongeldige beschuldigingen, te beweren dat er geen crisis is, of door een andere partij de schuld te geven van de crisis.

1. **Bolsterstrategie**

Deze strategie werkt door de organisatie te positioneren als een aanwinst voor haar stakeholders en hun aan zijn vroegere goede daden te herinneren. Verder worden stakeholders geprijsd en bedankt voor hun toewijding en loyaliteit. Een bolsterstrategie wordt vaak gebruikt in combinatie met andere primaire crisisstrategieën (zie tabel, Hoofdstuk III. 3.1 Identificeer uw instrumenten en middelen).

**Andere tips & tricks :**

* Interne sensibilisering: zorg ervoor dat iedereen binnen de organisatie het belang van goede voorlichting tijdens een crisis inziet.
* Opzet van een reactieketen bij een crisis (groot incident): wie zijn de betrokkenen en wat zijn hun verantwoordelijkheden?
* Oefen verschillende crisissituaties in via rollenspelen.
* Stel een crisismanagementplan (of incidentenbeheerplan) op en voorzie jaarlijks een update.
* Breng een natuurlijke samenwerking met de nodige (overheids)instanties tot stand.

Welke strategie u ook aanneemt, denk eraan: :

1. DEFINIEER HET INCIDENT.
   * Wat is er aan de hand? Welk incident heeft zich voor gedaan? Wat is de oorzaak?
2. ANALYSEER HET INCIDENT.
   * Hoe erg is het? Is er een invloed op cruciale bedrijfsprocessen?
3. DEFINIEER DE OPLOSSING.
   * Hoe lossen we het incident op? Wat moet er gebeuren?
   * Wat moet er eerst gebeuren? Prioriteer!
4. VERDELING TAKEN EN VERANTWOORDELIJKHEDEN.
   * De beheerder van de crisis bepaalt wie wat moet doen. Breng ook het personeel intern op de hoogte van de situatie.
5. COMMUNICEER EXTERN.
   * Contacteer de nodige instanties (bv. overheidsinstellingen, nutsbedrijven etc.) met als doel het probleem op te lossen. Verwittig indien nodig ook klanten, leveranciers en andere stakeholders.
6. FOLLOW-UP.
   * Eenmaal het incident is opgelost, doe een post incident review met als doel:
     1. Hoe kunnen we dit incident in de toekomst beter aanpakken &
     2. Hoe kunnen we dit incident in de toekomst vermijden?

Om snel en efficiënt te kunnen communiceren tijdens een crisissituatie, heeft u nood aan een **logische structuur in de berichtgeving**. Zo vergeet u geen belangrijke info en communiceert u to the point. De hierna uitgewerkte voorbeelden zijn een leidraad, maar kunnen uiteraard aangepast worden aan uw specifieke noden en aan de beschikbare communicatiekanalen.

|  |
| --- |
| **Element 1: Wat is er precies gebeurd?** |
| **Boodschap:** Omschrijf kort en feitelijk wat de situatie is. Blijf objectief en gis niet naar eventuele redenen of oorzaken indien deze nog niet gekend zijn. |

|  |
| --- |
| **Element 2: Wat is de impact voor uw doelgroep?** |
| **Boodschap:** Wat zijn de gevolgen voor uw doelgroep op dit moment? |

|  |
| --- |
| **Element 3: Wat doen hulpdiensten/crisismanagement/betrokken organisaties?** |
| **Boodschap:** Wat gebeurt er om de situatie onder controle te krijgen of te herstellen, wat zijn de next steps? |

|  |
| --- |
| **Element 4a: Wat moet ik wel doen?** |
| **Boodschap:** Vertel kort wat van de doelgroep verwacht wordt. |

|  |
| --- |
| **Element 4b: Wat moet ik niet doen?** |
| **Boodschap:** Vertel kort welke acties je wil vermijden en baken waar nodig verantwoordelijkheden af. |

|  |
| --- |
| **Element 5: Waar vind ik meer info?** |
| **Boodschap:** Wie is het aanspreekpunt binnen het bedrijf die deze crisis coördineert? Via welke kanalen zal de doelgroep op de hoogte gehouden worden en waar kan men terecht met vragen? |

|  |
| --- |
| **Element 6: Wanneer hoor ik meer?** |
| **Boodschap:** Maak een tijdsinschatting van wanneer een volgende communicatie zal volgen en via welke kanalen |

Om u te helpen, kunt u hieronder twee voorbeelden vinden van zowel interne als externe communicatie.

#### 1.3.1: Interne communicatie

*Voorbeeld CEO-fraude – preventieve oproep tot waakzaamheid*

*Hallo iedereen,*

*Vandaag hebben een aantal onder jullie deze mail ontvangen.*

***LET OP: Het gaat hier om zogenaamde* ***CEO-Fraude****, dit is een techniek waarbij oplichters zich voordoen als onze CEO Piet Vandamme, met als doel geld te laten overschrijven naar hun rekening.*

*Denk altijd goed na wanneer je zo’n mail ontvangt.*

*Check eerst en vooral het e-mailadres. Vaak lijkt dit in een eerste oogopslag correct, maar blijkt het bij nader onderzoek over een extern adres te gaan. (Tip: laat je cursor over de afzender zweven om het achterliggende adres te zien).Vraag je ook steeds af of wat men vraagt in de mail wel strookt met de geldende procedures.*

*Vraagt iemand van het management jou om een betaling te doen terwijl dit normaal niet tot jouw takenpakket behoort, of vraagt hij om hier zeker met niemand anders over te praten, check dan altijd via een ander kanaal of dit wel klopt!*

*In bijlage van deze mail vinden jullie ook een infofiche rond phishing en een fiche rond CEO-fraude met meer informatie.*

*Voor bijkomende vragen kunnen jullie steeds terecht bij Piet Janssens of de IT-afdeling.*

*Bedankt voor jullie oplettende medewerking,*

*Erin G. Trapp*

*Officemanager*

#### 1.3.2: Externe communicatie

*Voorbeeld waterlek - gebouwen ontoegankelijk*

*Beste klant,*

*Door de uitzonderlijk hevige regenval van afgelopen nacht is er water ingesijpeld op de 1e verdieping van het gebouw van <Bedrijfsnaam>. Een deel van het plafond is daarbij ingestort. Het serverlokaal is gevrijwaard, maar het merendeel van de bureaus zijn door het water en het ingezakte plafond voorlopig niet meer bruikbaar.*

*Daardoor is het bedrijfsgebouw momenteel NIET toegankelijk voor klanten en personeel.*

*De brandweer zal het gebouw deze voormiddag inspecteren, waarna een dakwerker de eerste herstellingen zal uitvoeren.*

*Ons personeel zal daarom voorlopig van thuis uit werken, uw vaste contactpersonen blijven beschikbaar via e-mail en gsm. Ook onze webshop blijft toegankelijk via www.NaamBedrijf.be. Geplande leveringen ondervinden weinig tot geen hinder van deze situatie.*

*We blijven u uiteraard op de hoogte houden van de evoluties*. *Een update van de situatie volgt morgen in de loop van de voormiddag via mail. Voor dringende vragen kan u steeds terecht op het nummer 04xx xx xx xx.*

*Met vriendelijke groeten,*

*Bart Waterman*

*Zaakvoerder*

## Stap 2: Melding en identificatie

2.1: Melding

Het is essentieel om een incident snel te kunnen opsporen, identificeren en kwalificeren/classificeren om de impact op de continuïteit van de activiteiten te beperken door de juiste procedure te activeren. De persoon die de melding van het incident ontvangt, kwalificeert het incident op van vooraf vastgestelde criteria.

Elke werknemer moet elk incident of gebeurtenis die tot een incident kan leiden, zo snel mogelijk melden. Klanten en leveranciers kunnen ook een incident melden.

De middelen om incidenten te melden zijn beschreven in het incidentenbeheerplan.

* Zie Stap 3: Activatie en behandeling, beheersmaatregelen

### 2.2: Identificatie

2.2.1: Identificeer de betrokken activiteiten

|  |
| --- |
| **Wat zijn de taken van het bedrijf die behouden moeten blijven om haar economische overleving te verzekeren?**  **Zie ook het Business Continuity plan (BCP) en de vastgelegde tijdsdoelstellingen (RTO,…)** |

Om u te helpen uw processen en activiteiten te prioriteren, stelt u zich de volgende vragen:

1. welke activiteiten zouden het personeel (of de klanten,...) in gevaar kunnen brengen?
2. welke activiteiten kunnen na enkele uren een ernstige economische impact hebben op het bedrijf? Na 24u? 48u? Een week?

**LIJST MET ESSENTIELE ACTIVITEITEN**

| **Essentiële activiteit 1** |
| --- |
| Sleutelpersoneel |
| Belangrijke informatie of gegevens |
| Noodzakelijke IT-diensten (hardware, software) |
| Gebouwen |
| Externe contactpersonen (ressources) |
| Onderlinge afhankelijkheid (interdependentie) met andere activiteiten (zo ja, welke) |
| ... |

2.2.2: Classificeer

De persoon die de informatie ontvangt (bv. Helpdesk) dient deze bijvoorbeeld als volgt in te delen:

1. **Zwak** - er hebben zich geen incidenten voorgedaan, maar de gebeurtenis houdt verband met een systeem, proces of organisatie en kan een incident in de nabije of toekomstige toekomst veroorzaken;
2. **Klein** - een incident dat geen significante impact heeft op de bedrijfscontinuïteit;
3. **Groot** - een incident dat een significante impact kan hebben op de organisatie, maar nog niet als een crisis wordt beschouwd;
4. **Crisis** - een incident dat een aanzienlijke impact kan hebben op de organisatie en de bedrijfscontinuïteit.

2.2.2: Identificeer de prioriteiten

|  |
| --- |
| In geval van onderbreking of achteruitgang van uw activiteiten, wat is de prioriteitsvolgorde van de activiteiten?  Wat zijn uw tijdsdoelstellingen?  Zie ook de Risk Assessment, Risk Treatment en het Business Continuity Plan |

Bij het analyseren van de impact op de bedrijfscontinuïteit moet u er rekening mee houden dat niet alle activiteiten noodzakelijkerwijs voor 100% werken, maar dat dit aanvaardbaar kan zijn.

Heeft u uw prioritaire activiteiten gedefinieerd? Nu gaat het erom de volgorde te bepalen waarin deze activiteiten moeten worden hervat (sommige diensten zijn onderling afhankelijk van andere) en de geschatte tijdsdoelstellingen te identificeren door ze te vergelijken met de vastgelegde doelstellingen (zie Risk Assessment en Business Continuity Plan).

Op basis van het bovenstaande, is het een kwestie van het bepalen in welke volgorde maatregelen moeten worden genomen om de continuïteit van essentiële activiteiten te waarborgen. Denk eraan de mogelijke onderlinge afhankelijkheid van bepaalde activiteiten te overwegen en een permanente dialoog met de beheerder van het Business Continuity Plan te onderhouden.

1. Stap 3: Activering en behandeling (INCIDENT)

### 3.1: Identificeer uw instrumenten en middelen

*Zie bijlage VII, punt 7.2: Tabel*

In het bijzonder uw procedures (identificatie,...), uw communicatiemiddelen,...

Het hoofddoel is om de impact van het incident zo snel mogelijk te verminderen voor de bescherming van het menselijk leven en vervolgens voor de continuïteit van de activiteiten van het bedrijf.

Welke strategie moet u nu hanteren bij welke crisis? Dat vindt u terug in de twee onderstaande tabellen, onderverdeeld in de primaire en de secundaire crisisresponsstrategie:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Strategietype** | **Crisistype** | **Strategische respons** | **Tactische actie** | **Beschrijving v/d tactische actie** |
| Primaire crisisresponsstrategie | Slachtoffercrisis | Ontkenstrategie | Val de aanklager aan | Confronteer de persoon/groep die beweert dat er iets mis is. |
| Ontkenning | Beweer dat er geen crisis is. |
| Zondebok | Geef een persoon of groep buiten de organisatie de schuld van de crisis. |
| Accidentele crisis | Inperkstrategie | Excuses | Minimaliseer uw verantwoordelijkheid door   * te ontkennen dat u de intentie had om schade te berokkenen; * te stellen dat u de oorzaak van de crisis niet kunt beheersen. |
| Rechtvaardiging | Minimaliseer de schade veroorzaakt door de crisis. |
| Te voorkomen crisis | Heropbouwstrategie | Compensatie | Geef een zekere compensatie (bv. geld of andere giften) aan de slachtoffers van de crisis |
| Verontschuldiging | Neem de volledige verantwoordelijkheid van de crisis en vraag om vergiffenis. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Strategietype** | **Strategische respons** | **Tactische actie** | **Beschrijving v/d tactische actie** |
| Secundaire crisisresponsstrategie | Bolsterstrategie | Herinnering | Vertel belanghebbenden over de waardevolle verwezenlijkingen van de organisatie uit het verleden. |
| Vleierij | Prijs belanghebbenden en herinner hen aan de waardevolle verwezenlijkingen van de organisatie uit het verleden. |
| Slachtofferschap | Herinner belanghebbenden eraan dat de organisatie ook het slachtoffer is van de crisis. |



#### **3.2: BEHEERSMAATREGELEN**

|  |  |
| --- | --- |
|  | **DO’s** |
|  | **Communiceer eerst intern** (eigen medewerkers) en naar alle betrokkenen (stakeholders, partners, leveranciers ... ), dan pas naar buiten. |
|  | **Beperk u tot de feiten.** Zorg dat uw informatie juist is en zo volledig mogelijk. |
|  | Verspreid de boodschap via **verschillende kanalen**. U verhoogt de kans dat mensen ze horen, ze sneller aanvaarden en dat ze blijft hangen. |
|  | De manier waarop u communiceert met personeel, stakeholders, pers … hangt af van **de aard van de crisis**. Het is tijd om uw voorbereide boodschappen boven te halen en ze aan te passen aan de situatie! |
|  | **Stel de mensen gerust** **en geef raad**. |

|  |  |
| --- | --- |
|  | DONT’S |
|  | **Laat u niet pakken in snelheid.** Hoe sneller u communiceert, hoe minder ruimte u laat voor speculatie en roddels. Een snelle reactie is niet hetzelfde als een emotionele of geïmproviseerde reactie. |
|  | **Vergeet geen doelgroepen**: denk ook aan de pers, andere betrokkenen, geïnteresseerde derden zoals buren. |
|  | Handel het incident niet zakelijk en zonder emotie af. **Maar** **laat de emoties ook niet de overhand nemen**. |
|  | **Beantwoord nooit onmiddellijk** **[telefoons van journalisten](https://www.klasse.be/74280/hoe-ga-je-om-met-de-pers-bij-crisis-op-school/" \t "_blank)**. Laat iemand de telefoons aannemen, de gegevens van de journalist noteren en wat hij wil weten. **Bel een kwartier later terug en bereid u voor.** |
|  | **Wees open en eerlijk, maar geef niet alle details vrij.** Respecteer altijd de integriteit en privacy van de betrokkenen. Geef nooit vertrouwelijke informatie door. |

## Stap 4: Eradication

Het is niet altijd mogelijk om de oorzaken van het incident tijdens het incident zelf vast te stellen. In dit geval moeten eerst de gevolgen (impact op de bedrijfscontinuïteit) worden aangepakt voordat de oorzaak kan worden vastgesteld. Er moeten echter redelijke inspanningen worden geleverd om de oorzaak te achterhalen en het risico te beperken dat een dergelijk incident zich opnieuw voordoet

1. Stap 5: Deactivering

Wanneer de diensten die door een incident werden getroffen, weer normaal functioneren, kan het incident worden afgesloten door het team dat het incident opvolgde (bv. helpdesk) in overeenstemming met de beheerder van het Business Continuity Plan.

Het incidentenbeheerplan wordt gedeactiveerd en er wordt een "Post Incident Review" uitgevoerd (zie stap 6).

De volgende acties moeten worden ondernomen:

| **Actie** | **Functie** | **Verwijzingen naar andere documenten**  **Naam en referentie** |
| --- | --- | --- |
| Afsluiten van het incidententicket | Helpdesk na akkoord van de beheerder van het incidentenbeheerplan | Ticket in het kader van incidentenbeheer |
| Deactiveren incidentenbeheerplan | Beheerder incidentenbeheerplan |  |
| Post Incident Review | Beheerder incidentenbeheerplan | Post Incident Review (document) |
| … |  |  |

1. Stap 6: Geleerde lessen (Post Incident Review) (NA HET INCIDENT)

*“I never lose. I either win or learn.”*

Nelson Mandela

Het doel is om te leren van haar ervaring door het uitvoeren van een "post incident review" om het incident management in een continu proces te verbeteren.

De Post Incident Review moet ten minste de volgende elementen bevatten:

6.1: Context: verzamel de juiste informatie

| **Element** | **Informatie** |
| --- | --- |
| **Administratie** |  |
| Incidentnummer in het incidentlogboek: |  |
| Datum en tijd waarop het incident werd vastgesteld: |  |
| Datum en tijd waarop het incident werd opgelost: |  |
| Type incident: |  |
| Ernst van het incident: |  |
| Was er impact voor klanten: |  |
| Wie was beheerder van het incident: |  |
| Beschrijving van het incident: |  |
| … |  |

6.2: Evaluatie van het incident en geleerde lessen

|  |  |
| --- | --- |
| **Detectie** |  |
| Wie stelde het incident vast en hoe: |  |
| Werd het incident tijdig opgemerkt of had het eerder ontdekt kunnen worden: |  |
| Kunnen procedures of tools helpen om dit soort incidenten nog vroeger op te sporen: |  |
| Werden de juiste meldingsprocedures gevolgd: |  |
| … |  |

|  |  |
| --- | --- |
| **Beoordeling en acties** |  |
| Werd het incident correct ingeschat: |  |
| Was de hiervoor nodige informatie beschikbaar: |  |
| Werd het BCP geactiveerd: |  |
| Welke andere acties werden ondernomen om het incident op te lossen: |  |
| Welke resources werden gebruikt om het incident te beheren: |  |
| Is het plan flexibel genoeg om met onvoorziene events om te kunnen gaan: |  |
| Werden de acties tijdig ondernomen: |  |
| … |  |

|  |  |
| --- | --- |
| **Communicatie** |  |
| Werd er (tijdig) intern gecommuniceerd: |  |
| Werd er (tijdig) extern gecommuniceerd: |  |
| Welke communicatiekanalen werden ingezet: |  |
| Wanneer werd de eerste communicatie uitgestuurd en hoe regelmatig werd deze geüpdatet: |  |
| Werden de juiste personen betrokken: |  |
| Welke communicatie was nuttig: |  |
| Welke communicatie bleek inefficiënt: |  |
| … |  |

|  |  |
| --- | --- |
| **Analyse van de oorzaak** |  |
| Werd de oorzaak van het incident vastgesteld: |  |
| Zijn er verwante of soortgelijke incidenten vastgesteld: |  |
| Is er een onderliggend probleem: |  |
| Is er extra actie nodig om het onderliggende probleem te identificeren (zie stap 4 Eradication): |  |
| … |  |

|  |  |
| --- | --- |
| **Preventie** |  |
| Wat kunnen we leren uit de gebeurtenis: |  |
| Hoe kunnen we vermijden dat een soortgelijk incident zich opnieuw voordoet, en wie moet hiervoor actie ondernemen: |  |
| … |  |

|  |  |
| --- | --- |
| **Gepastheid van de reactie** |  |
| Effectieve hersteltijd (vergelijk met Recovery Time Objective – RTO)  Het incident werd binnen de vooropgestelde tijd opgelost:  Voor geen van de activiteiten  Slechts voor enkele activiteiten  Voor alle activiteiten |  |
| Moeten er contracten aangepast worden: |  |
| … |  |

|  |  |
| --- | --- |
| **Hoe reageerde het management op het incident** |  |
| Management reageerde niet of onvoldoende |  |
| Management reageerde, maar volgde de plannen niet volledig |  |
| Management reageerde volledig volgens de plannen |  |
| … |  |

|  |  |
| --- | --- |
| **Mate waarin het personeel voorbereid was op het incident** |  |
| 1. Onvoorbereid |  |
| 2. Deels voorbereid |  |
| 3. Volledig voorbereid |  |
| … |  |

|  |  |
| --- | --- |
| **Gewenste verbeteringen** |  |
| Wat zou kunnen bijgestuurd worden om het incident in de toekomst sneller op te lossen: |  |
| … |  |

|  |  |
| --- | --- |
| **Schadeclaims** |  |
| Zijn er schadeclaims: |  |
| Werden schadeclaims ingediend bij derden in verband met dit incident: |  |
| … |  |

|  |  |
| --- | --- |
| **Varia** |  |
| … |  |

## Bijlagen

7.1: Contactenlijst

**INTERNE CONTACTEN**

| **Functie** | **Voornaam NAAM**  ***Denk eraan om ook een andere persoon aan te duiden in geval van afwezigheid, ziekte,... van de referentiepersoon.*** | **Actie** | **Contactgegevens**  ***Vaste telefoon***  ***Bureau***  ***Thuis***  ***Mobiel***  ***E-mail***  ***Voorkeuren voor contact (snelste)*** |
| --- | --- | --- | --- |
| Referentiepersoon (bedrijfscontinuïteit) |  |  |  |
| Alternatief |  |  |  |
| ... |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**EXTERNE CONTACTEN**

| **Functie** | **Voornaam NAAM**  ***Denk eraan om ook een andere persoon aan te duiden in geval van afwezigheid, ziekte,... van de referentiepersoon.*** | **Contract**  ***Referentie*** | **Contactgegevens**  ***Vaste telefoon***  ***Bureau***  ***Thuis***  ***Mobiel***  ***E-mail***  ***Voorkeuren voor contact (snelste)*** |
| --- | --- | --- | --- |
|  |  |  |  |
| Journalisten |  |  | Vaste telefoon  Bureau  1)  2)  Thuis  1)  2)  Mobiel  1)  2)  E-mail  1)  2) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| … |  |  |  |
| … |  |  |  |

7.2: Tabel

|  |  |  |
| --- | --- | --- |
| **1.1: Kies iemand die aan het roer staat** | **Functieomschrijving van wie de taak uitvoert** | **Welke procedures moeten gevolgd worden?** |
|
| [Scenario 1] |  |  |
| [Scenario 2] |  |  |
| […] |  |  |

|  |  |  |
| --- | --- | --- |
| **1.2: Ken uw risico’s** | **Herneem het resultaat uit kolom P van de Risk Assessment (2 (groen) tot 10 (rood))** | **Focusgroep?** **(1 of 2)** |
| O.b.v. uw Risk Assessment, wat is uw risiconiveau in scenario 1? |  |  |
| O.b.v. uw Risk Assessment, wat is uw risiconiveau in scenario 2? |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **2.2.3: Identificeer de prioriteiten**   * Wat zijn uw tijdsdoelstellingen? * Wat is de maximale "aanvaardbare" tijd voor u om de werking van de activiteit te herstellen? (Recovery Time Objective of RTO) * Wat is de maximale leeftijd van de gegevens die u nodig heeft om te herstellen (Recovery Point Objective of RPO) * Wat heeft u met uw leveranciers afgesproken (Recovery Consistency Objective of RCO)? * … in geval van onderbreking of verslechtering van uw activiteiten, wat is de prioriteitsorde van de activiteiten (P)? | | | |
| **2.2.1: Identificeer de betrokken activiteiten** |  | | **RTO** | **RPO** | **RCO** | **P** |
| Mensen |  | |  |  |  |  |
| Infrastructuur |  | |  |  |  |  |
| Technologie |  | |  |  |  |  |
| Informatie en documentatie |  | |  |  |  |  |
| Derden |  | |  |  |  |  |
| … |  | |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **3.1: Identificeer uw instrumenten en middelen** | **Essentiële activiteit 1** | **Essentiële activiteit 2** |
| Sleutelpersoneel |  |  |
| Belangrijke informatie of gegevens |  |  |
| Noodzakelijke IT-diensten (hardware, software) |  |  |
| Gebouwen |  |  |
| Externe contactpersonen (middelen) |  |  |
| Interdependentie met andere activiteiten (zo ja, welke) |  |  |
| **…** |  |  |