

TELECOMMUNICATIE

CATEGORIE: Technologische afhankelijkheid

 In samenwerking met :

# 

# Telecom

De digitale transitie die onze samenleving momenteel doormaakt, is gebaseerd op telecommunicatie en biedt veel *opportuniteiten* voor bedrijven. Zij ontwikkelen meer en meer digitale strategieën om zich te kunnen positioneren in een markt die openstaat voor de wereld.

Bij de ontwikkeling van dergelijke strategieën is het echter belangrijk om de risico's niet te onderschatten. Wordt de geplande digitalisering op een cyberveilige manier uitgevoerd? Zijn de aspecten met betrekking tot de bescherming van de persoonlijke levenssfeer en persoonsgegevens naar behoren beoordeeld (GDPR,...)? Zijn de wettelijke verplichtingen met betrekking tot de informatie die op websites moet worden opgenomen, nageleefd? Is het personeel voldoende getraind en op de hoogte?...

Naast deze risico's die inherent zijn aan elke online activiteit, is er ook het risico van technologische afhankelijkheid: het bedrijf is steeds meer afhankelijk van telecommunicatie (internet, mobiele telefonie, vaste telefonie) voor zijn goede werking. Denk maar aan betaalmiddelen, het beheer van de logistieke keten, klantenrelaties, personeelsbeheer, contacten met leveranciers, de verwerking van dossiers, het beheer van online reputatie,…

Daarom is het belangrijk om het risico van een onderbreking van de telecommunicatiemiddelen te evalueren en wat dit concreet voor uw bedrijf zou kunnen betekenen. Kan uw bedrijf omgaan met een aanzienlijke onderbreking of verslechtering van de telecommunicatiemiddelen?

**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 interpretaties in concrete gevallen of situaties kan altijd het advies worden ingewonnen van de ambtenaren die verantwoordelijk zijn voor het toezicht op de arbeidsveiligheidsvoorschriften.

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

TELECOMMUNICATIE

[I. Stap 1: Voorbereiding (VOOR HET INCIDENT) 4](#_Toc57970032)

[1.1: Kies iemand die aan het roer staat 4](#_Toc57970033)

[1.2: Ken uw risico’s 4](#_Toc57970034)

[1.3: Preventieve maatregelen 5](#_Toc57970035)

[II. Stap 2: Melding en identificatie 7](#_Toc57970036)

[2.1: Melding 7](#_Toc57970037)

[2.2: Identificatie 7](#_Toc57970038)

[III. Stap 3: Activering en behandeling (INCIDENT) 8](#_Toc57970039)

[3.1: Identificeer uw instrumenten en middelen 8](#_Toc57970040)

[3.2: **BEHEERSMAATREGELEN** 9](#_Toc57970041)

[IV. Stap 4: Eradication 10](#_Toc57970042)

[V. Stap 5: Deactivering 10](#_Toc57970043)

[VI. Stap 6: Geleerde lessen (post incident review) (NA HET INCIDENT) 11](#_Toc57970044)

[6.1: Context : verzamel de juiste informatie 11](#_Toc57970045)

[6.2: Evaluatie van het incident en geleerde lessen 11](#_Toc57970046)

[VII. Bijlagen 15](#_Toc57970047)

[7.1: Contactenlijst 15](#_Toc57970048)

[7.2: Tabel 17](#_Toc57970049)

## 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).

Vergeet niet uw interne of externe IT-dienst als u die heeft.

Zorg ervoor dat u de procedures/het incidentbeheerplan 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 zijn, moet het bedrijf haar risico's hebben geïdentificeerd, geanalyseerd en geëvalueerd. Dit is het doel van de Risk Assessment (zie template). Het is ook noodzakelijk dat de maatregelen voor het behandelen van deze risico’s gekend zijn, dit is het doel van de Risk Treatment (zie template).

Gezien de grote afhankelijkheid van onze maatschappij van telecommunicatie, kan iedereen snel de gevolgen voelen van een aanzienlijke verslechtering of onderbreking van de telecommunicatiediensten en de impact ervan op de bedrijfscontinuïteit.

Afhankelijk van de activiteiten van het bedrijf, kan het zijn dat u verstoringen ondervindt zoals :

* moeilijkheid om contact op te nemen met leveranciers en klanten,
* ontoegankelijke databases,
* (sterke) verslechtering of onderbreking van de online klantenservice,
* gevolgen voor de logistieke keten, verslechtering of onderbreking van online activiteiten,
* schade aan de reputatie,
* het niet halen van termijnen,
* verstoorde commandoketen,
* ...

De sterke verstoring van de telefoonlijnen kan verschillende oorzaken hebben: een storm, een stroomonderbreking, een abnormale toestroom van oproepen (na een aanslag in de buurt bijvoorbeeld), ...

Vergeet niet dat een Risk Assessment (zie template) een iteratief proces is en niet één enkele handeling. Telecomnetwerken, uw behoeften en uw risico's evolueren voortdurend.

Specifieke scenario's moeten in kaart gebracht worden. Bijvoorbeeld :

##### Scenario 1. Mobiele of vaste telefonie

Het bedrijf heeft geen toegang meer tot vaste of mobiele telefoondiensten. Dit scenario kan al dan niet gepaard gaan met een verlies van de internetverbinding.

In het geval van een stroomstoring is het ook mogelijk dat de vaste telefonie eerst uitvalt en dan, na enkele uren, dat uw toestel of de antennes die u bedienen geen batterij meer hebben.

##### Scenario 2. Internetverbinding

Het bedrijf ervaart een sterke degradatie van zijn internetverbinding of heeft geen toegang meer tot het internet. Het is mogelijk dat de middelen voor toegang tot het internet via de smartphone blijven bestaan, maar de toegang tot de tools van het bedrijf (database, specifieke software, enz.) kan hierdoor moeilijk of zelfs onmogelijk zijn.

1.3: Preventieve maatregelen

##### Scenario 1: Mobiele of vaste telefonie

**Redundantie**

Als de impact van een storing in de vaste en/of mobiele telefonie op het bedrijf aanzienlijk kan zijn, denk er dan aan om effectieve redundatieregelingen te voorzien (back-up). U kunt bijvoorbeeld twee concurrerende (redundante) vaste telefoonlijnen hebben of twee verschillende simkaarten. Deze redundantie kan door verschillende concurrerende operatoren (ten minste 2) worden aangeboden.

Als het om vaste telefonie gaat, vergeet dan niet aan uw operatoren te vragen of één van hen zijn infrastructuur huurt van een andere operator om u te bedienen: het is mogelijk dat uw gebouw wordt bediend door één en dezelfde "kabel". Als dit het geval is, zou u twee keer betalen, maar zonder over eigenlijke redundantie te beschikken.

**Plan "B"**

Intern

Denk eraan om alle interne procedures te identificeren, alsook alle commandoketens (technici, IT, management, enz.) die afhankelijk zijn van de toegang tot telecommunicatiemiddelen (vaste en mobiele telefonie en internet) voor hun goede werking. Vergeet niet om alternatieve middelen voor deze procedures en commandoketens te identificeren in geval van verlies van telecommunicatiemiddelen. Vermenigvuldig de mogelijke communicatiekanalen en als geen van deze kanalen meer toegankelijk zijn, vergeet dan niet uw instructies aan te geven (telewerken,....).

Extern

Vergeet ook niet om uw klanten en leveranciers verschillende mogelijkheden te geven om contact met u op te nemen.

Nuttige links

* [FOD Economie](https://economie.fgov.be/nl/themas/energie/bevoorradingszekerheid/elektriciteitsschaarste/veelgestelde-vragen/veelgestelde-vragen-door)
* [BE-Alert](https://be-alert.be/nl)

##### Scenario 2: Internetverbinding

**Redundantie**

Als de impact van een storing in de internetverbinding op het bedrijf aanzienlijk kan zijn, denk er dan aan om effectieve redundantieregelingen te voorzien (back-up). U zou bijvoorbeeld twee concurrerende (redundante) verbindingen kunnen hebben. Deze redundantie kan door verschillende concurrerende operatoren worden aangeboden (ten minste 2).

Vergeet niet aan uw telecomoperator, betalingsdienst,... te vragen:

* Of hij, om u van dienst te zijn, de infrastructuur geheel of gedeeltelijk huurt van een andere operator. Indien dit het geval zou zijn, dan kunt u nl. twee contracten hebben met twee verschillende operators, maar...met eenzelfde aansluiting. Als deze zou falen, dan heeft u geen echte back-up. Effectieve redundantie betekent dat u beschikt over meerdere afzonderlijke verbindingen die niet van elkaar afhankelijk zijn.
* Of uw operator u kan vertellen wat het percentage van de bereikbaarheid tijdens uw werkuren is en wat de maximale tijd van onderbreking of verstoring is die de afgelopen 12 maanden werd geregistreerd.
* Of de infrastructuur die uw operator u aanbiedt "Single Points of Failure" (SPoF) bevat, d.w.z. punten die geen redundantie hebben.
* Indien u de toegang tot elektriciteit zou verliezen, hoelang u dan geen toegang meer zou hebben tot het internet? Biedt uw telecomoperator u oplossingen? Informeer naar de werking van het netwerk van de exploitant in de "last miles", de mogelijkheid om omvormers te leveren,…
* Of u kunt profiteren van 24/7 helpdeskondersteuning.

**Veerkracht van het netwerk (contracten)**

Uw contracten moeten "service level agreements" (SLA's) bevatten die ten minste enkele aspecten met betrekking tot de veerkracht van het netwerk identificeren. Denk er m.n. aan te eisen naar:

* Een gegarandeerde beschikbaarheid (%)
* Probleemoplossingstijden in relatie tot de door u gedefinieerde tijdsdoelen (zie 2.2.3)
* Implementatie van back-upoplossingen (zie commentaar op de daadwerkelijke effectiviteit van deze maatregel)
* U kunt ook bepaalde middelenverbintenissen (uw operator doet "wat hij kan") omzetten in een resultaatsverbintenis (indien het resultaat niet wordt bereikt, worden er geldboetes voorzien).
* ...

## 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: Activering 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.

2.2.3: 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)

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

3.1: Identificeer uw instrumenten en middelen

*Zie bijlage VII, punt 7.2: Tabel*

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

### 3.2: BEHEERSMAATREGELEN

##### Scenario 1: Mobiele of vaste telefonie

##### Scenario 2: Internetverbinding

De meeste maatregelen die u kunt nemen zijn preventieve maatregelen. Als het incident er is, heeft u nog maar een klein beetje speelruimte...

In beide scenario's kunnen de volgende reflexen u helpen:

**Denk aan het evidente**

* Controleer of alle kabels, routers en modems goed zijn aangesloten en of de stroomvoorziening goed is.
* Controleer of u het wifinetwerk niet heeft afgesloten (knop, sleutel, ...).
* Controleer of andere websites nog steeds toegankelijk zijn (het probleem is misschien niet uw verbinding, maar de site die u wilt bezoeken).

**Denk aan uw IT-tools**

* Controleer of uw firewall werkt en niet alle verkeer blokkeert.
* Vernieuw uw IP-adres (vergeet niet de nodige [informatie](https://www.tp-link.com/nl-be/support/faq/840/) af te drukken als u niet weet hoe u dit moet doen).
* Reset uw toestellen (modems,....): als u de "reset"-knop niet kunt vinden, haal dan de stekker van de modem uit het stopcontact gedurende minstens 30 seconden voordat u deze weer aansluit.

**Controleer bij de buren** of dit een probleem is dat ook hen treft of dat u de enige bent die erdoor getroffen wordt..

Indien mogelijk, **neem contact op met uw telecomoperator**

Als het na een paar minuten nog steeds niet werkt, neem dan contact op met uw professionele (niet "residentiële") klantenservice.

**Ga verder met Plan B**

Gebruik, indien mogelijk, tijdelijk andere communicatiemiddelen en denk eraan om het personeel te informeren.

**Denk aan uw externe communicatie**

Klanten, leveranciers die misschien overstuur raken? Zie Fiche Communicatie.

1. 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 uit de ervaring door een "Post Incident Review" uit te voeren en zo het incidentenbeheer via een continu proces te verbeteren.

De Post Incident Review zou ten minste de volgende elementen moeten 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** |  |
| … |  |

1. 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)*** |
| --- | --- | --- | --- |
| Verzekeraar |  |  | 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) |  |  |
| **…** |  |  |