Crisis
Management Plan

Documentgeschiedenis

**GESCHIEDENIS WIJZIGINGEN**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Gewijzigd door** | **Omschrijving van de wijzigingen** |
| **xxx** | **xxx** | **xxx** | **xxx** |
|  |  |  |  |
|  |  |  |  |

**GESCHIEDENIS GOEDKEURINGEN**

|  |  |  |
| --- | --- | --- |
| **Naam** | **Functie** | **Datum goedkeuring** |
| **xxx** | **xxx** | **xxx** |
|  |  |  |
|  |  |  |

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

Dit document wordt als volgt bewaard:

* In papieren vorm op volgende locaties: **[lijst locaties]**.
* 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](#_Toc56789805)

[**Hoofdstuk II Structuur voor Crisis Management** 5](#_Toc56789806)

[2.1. Continuïteitsprobleem/ major incident 6](#_Toc56789807)

[2.2. Crisis Management Team 6](#_Toc56789808)

[2.3. Inroepen van het Crisis Management Plan 8](#_Toc56789809)

[**Hoofdstuk III Crisis Management Plan** 9](#_Toc56789810)

[3.1. Een Crisis analyseren, isoleren en herstellen 9](#_Toc56789811)

[3.2. Deactivatie en post-crisis review 10](#_Toc56789812)

[**Hoofdstuk IV CMT-meeting locaties**  11](#_Toc56789813)

[4.1. Conference calls 11](#_Toc56789814)

[4.2. Hoofdlocatie 11](#_Toc56789815)

[4.3. Backup locaties 11](#_Toc56789816)

4.3.[1 – locatie [A] 11](#_Toc56789817)

4.3.[2 – locatie [B] 12](#_Toc56789818)

[**Hoofdstuk V Goedgekeurde manieren van communiceren**  13](#_Toc56789819)

[**Hoofdstuk VI Cruciale data**  14](#_Toc56789820)

[6.1. Locaties van activa 14](#_Toc56789821)

[6.2. Overzicht en locatie van relevante plannen 14](#_Toc56789822)

[6.3. Voorbereide verklaringen en communicatieboodschappen 15](#_Toc56789823)

[**Hoofdstuk VII Bijlagen** 16](#_Toc56789824)

[7.1. Appendix 1 – contactgegevens noodgevallen 16](#_Toc56789825)

[7.1.1. Crisis Management Team 16](#_Toc56789826)

[7.1.2. Andere (overheid, leveranciers, handelaars, …) 17](#_Toc56789827)

[7.2. Appendix 2 – bijhorende documenten 17](#_Toc56789828)

Hoofdstuk I
Doel van het document

**Het doel van een Crisis Management Plan (CMP) is** om de nodige maatregelen vast te leggen om ervoor te zorgen dat crisissen in uw bedrijf zo goed mogelijk kunnen worden aangepakt. Dit helpt om risico’s te beperken, inkomsten te beschermen en klantenvertrouwen te bewaren.

Het CMP zorgt voor een kader waarin crisissen zo efficiënt mogelijk kunnen worden aangepakt. Het moet gezien worden als een hulpmiddel om crisissen te beheren. Het CMP alleen zal evenwel geen crisissen oplossen en heeft niet als doel om concrete oplossingen voor alle mogelijke scenario’s voor te stellen. *Daarom is het belangrijk om het CPM te gebruiken in combinatie met het Business Continuity Plan of andere plannen die binnen uw bedrijf gebruikt worden.*

Het CMP is bedoeld voor crisissituaties die een impact hebben op uwbedrijf en die een gecoördineerde aanpak vereisen over verschillende afdelingen. Het CMP wordt niet ingeschakeld bij bedrijfsspecifiek crisissen die het best door de bedrijfsleiding afgehandeld kunnen worden. Herstelmaatregelen van puur operationele aard vallen niet onder de scope van dit document.

Het Crisis Management Plan wordt geactiveerd in situaties waarbij:

* Belangrijke delen van de werking van het bedrijf of de veiligheid van het personeel bedreigd worden.
* Snelle beslissingen van het topmanagement noodzakelijk zijn.
* Meerdere afdelingen en divisies gecoördineerd moeten samenwerken.

Een crisis kan zich zowel plots voordoen als geleidelijk aan groeien. Een crisis kan veroorzaakt worden door tal van interne als externe factoren en kan zowel materiële als immateriële schade veroorzaken.

Voorbeelden van crisissen zijn:

* Langdurige uitval van datanetwerken.
* Diefstal van data of cybercriminaliteit.
* Onbeschikbaarheid belangrijke delen van de infrastructuur.
* Faillissement of problemen bij externe leveranciers
* Sociale onrust.
* Ernstige negatieve persaandacht.
* Epidemie.
* Fraude.
* …

**Het Crisis Management Plan moet minstens tweejaarlijks getest worden, door zowel de leden als back-up leden.**

Hoofdstuk II
Structuur voor Crisis
Management

Om ervoor te zorgen dat dit plan efficiënt kan zijn, moeten alle maatregelen en afspraken in het plan grondig voorbereid en ingeoefend worden.

Alle betrokkenen bij dit plan moeten op de hoogte zijn van de rol die ze hierin spelen.

Crisissen binnen de organisatie kunnen aangepakt worden op 2 niveaus. Beide niveaus hebben hun eigen specifieke focus en rolverdeling.

Afhankelijk van de aard van de crisis en het niveau waarop deze wordt aangepakt, zullen de betrokken partijen binnen het **Crisis Management Team** (CMT) variëren. Het is belangrijk om alle stakeholders te betrekken in functie van de situatie.

Afdeling
X / BU X

Continuïteitsprobleem /
Major Incident

**Afdeling**
1 / BU 1

\*Business Unit

Afdeling
4 / BU 4

**Coördinatie op bedrijfsniveau, over verschillende afdelingen heen**

**Coördinatie op afdelingsniveau, bedrijfsleiding is op de hoogte**

**Afdeling**
2 / BU 2

**Afdeling**
3 / BU 3

Crisis

## 2.1. Continuïteitsprobleem/ major incident

Een continuïteitsprobleem of een major incident wordt **afgehandeld en beheerd door het Business Continuity Plan (of procedures voor major incidenten) binnen een afdeling, maar omwille van de ernst van de situatie is het belangrijk dat ook management buiten de afdeling op de hoogte is.** Het team dat instaat voor het behandelen van deze situaties (vaak het Business Continuity Team genoemd in Business Continuity Plannen) bestaat uit alle werknemers die het aanpakken van deze major incidenten mee aansturen.

Hierbij wordt doorgaans het “major incident process” gevolgd om crisissituaties aan te pakken op afdelingsniveau zonder dat coördinatie op bedrijfsniveau nodig is. (Indien het incident niet gekwalificeerd wordt als “major”, zie template IRP).

## 2.2. Crisis Management Team

Het CMT wordt samengesteld voor het aanpakken van een crisis die coördinatie vereist over verschillende afdelingen of businessunits (BU) heen. Het CMT staat doorgaans in voor:

* Strategische en tactische coördinatie over de verschillende afdelingen heen.
* Het verzamelen en delen van informatie.
* Het formuleren van opties en beslissingen die genomen worden binnen een crisis management strategie.

Alle **CMT-leden** dragen actief bij tot de aanpak van een crisis en overleggen en analyseren de situatie terwijl ze in nauw contact staan met hun **respectievelijke (Business Continuity) Teams**.

De volgende **crisismanagement** rollen vormen de kern van het crisisteam:

| Rol | Verantwoordelijkheden |
| --- | --- |
| Crisis Manager | * Starten en beëindigen van het crisismanagement proces.
* Sameroepen en voorzitten van CMT-meetings.
* Zorgen dat de juiste functies aanwezig zijn bij de CMT-meetings.
* Analyseren en beoordelen van het incident.
* Zorgen dat alle cruciale beslissingen tijdig genomen worden.
* Prioriteiten stellen indien nodig.
* Finale beslissingen nemen in geval van conflict binnen het CMT tijdens een crisis.
 |
| Vertegenwoordiger(s) getroffen afdelingen | * Rapporteren over ernstige problemen en de status van bedrijfsprocessen.
* Begeleiden en aansturen van inspanningen om de werking te herstellen in geval van een crisis.
* Ondersteunen van het CMT met analyses en advies.
* Inschatting haalbaarheid van voorgestelde alternatieven/ herstelopties.
* Inschatten en uitvoeren van herstelmaatregelen voor bedrijfsprocessen.
 |
| Communicatieadviseur | * Adviseren over de te volgen communicatiestrategie op zowel bedrijfs- als afdelingsniveau, waar nodig.
* Coördinatie van interne en externe communicatie tijdens een crisis.
* Rapporteren van pers- en social media coverage.
* Actief aansturen van interne communicatie in samenwerking met HR.
* Voorbereiden van de leden van het Directiecomité en/of Raad van Bestuur voor publieke communicatie en verklaringen.
 |
| HR-afgevaardigde | * In overleg met communicatieadviseur collega’s tijdig informeren.
* Aanpakken van personeel gerelateerde kwesties in crisissituaties.
* Zorgen voor coördinatie en advies met betrekking tot vragen, richtlijnen en communicatie met medewerkers.
 |
| Facilitair adviseur (indien vereist) | * Informatie verzamelen van veiligheids- en hulpdiensten waar nodig.
* Communiceren van de actuele veiligheidssituatie.
* Zorgen dat beschadigde of geëvacueerde gebouwen worden beveiligd.
* Zorgen voor alternatieve voorzieningen indien nodig.
 |
| Bedrijfsjurist (indien vereist) | * Monitoren van en rapporteren over legale kwesties.
* Inschatten en adviseren van het CMT rond legale kwesties of voorgestelde oplossingen.
 |
| Risk & Security afgevaardigde | * Monitoren, rapporteren en adviseren van het CMT over risico-gerelateerde aspecten.
* Bijstaan van de Crisis Manager tijdens het crisismanagement proces.
* Zorgen dat alle geïdentificeerde issues tijdens een crisis worden vastgelegd voor een post-crisis review en voortdurend verfijnen van het CMP.
 |
| Verbindingsofficier met overheid/ regulator (indien vereist) | * Monitoren en aanpakken van aspecten die vereist zijn door de overheid.
* Aandachtig monitoren van zaken waarvoor interactie met de overheid vereist is.
 |
| Secretaris/-esse | * Vastleggen van beslissingen genomen tijdens CMT meetings.
* Meeting-verslagen van CMT meetings bijhouden.
 |
| … |  |

Waar nodig en afhankelijk van de specifieke situatie, kunnen andere functies gevraagd worden om deel uit te maken van het CMT.

*Vul aan op basis van uw specifieke bedrijfssituatie: bv. Veiligheid & Preventie, Product & Services specialisten, Derden, …).*

**Elk lid van het CMT** moet:

* Zorgen voor strategisch leiderschap tijdens een crisis.
* Deelnemen aan CMT-meetings en hun respectievelijke afdelingen op de hoogte houden.
* In staat zijn om waar nodig beslissingen te nemen tijdens de CMT-meeting.
* Ervoor zorgen dat beslissingen genomen tijdens een CMT-meeting gecommuniceerd en uitgevoerd worden binnen hun respectievelijke organisaties en daarbuiten.

## 2.3. Inroepen van het Crisis Management Plan

Een crisis kan zichzelf plots voordoen op geleidelijk evolueren en escaleren. Wanneer een incident als “major” beschouwd wordt, dan kan een major incident/ Business Continuity Team binnen elke afdeling ingeroepen worden om major incidenten en crisissituaties te beheren in lijn met de incident managementprocessen. Voor kleinere incidenten: zie template IRP.

Zodra een afdeling de inschatting maakt dat een meer formele aanpak over verschillende afdelingen noodzakelijk is om de crisis het hoofd te bieden, kan ze beslissen om de crisis te escaleren naar bedrijfsniveau en het CMT te activeren.

Deze beslissing kan worden genomen door het hoofd van de afdeling of een gemachtigde afgevaardigde**.** (zie ook bijlage 1)

**Crisis
Manager**

**CEO**

**Afdelingshoofd of gemachtigd afgevaardigde**

**Afdeling**

**Inroepen Crisis Management Plan**

Business Continuity /
Major Incident Management

Activeren CMP?

Contacteren CEO

Aanstellen Crisis Manager

Samenroepen CMT en toepassen CMP

Einde incident & incident process

Einde crisis &
CMP

CMT meetings

Major Incident

Hoofdstuk III
Crisis Management Plan

In het geval van een crisis die coördinatie op bedrijfsniveau vereist, zal zo snel mogelijk een meeting van het CMT samengeroepen worden. De calls/meetings moeten verlopen volgens het hieronder beschreven proces (Hoofdstuk III) en agenda (Bijlage VII, 7.3).

De snelheid waarmee een incident zich voordoet, zal de frequentie van de CMT-meetings bepalen, dit kan variëren van dagelijks tot 1 maal per uur in gevallen waarin het incident snel evolueert. Daarnaast worden CMT-meetings vaak frequenter gehouden een het begin dan aan het eind van een crisis.

De cyclus van het crisismanagement wordt herhaald zo lang dat nodig is voor de specifieke crisis. De Crisis Manager beslist wanneer geen verdere CMT-meetings meer nodig zijn om de situatie aan te pakken.

De Crisis Management Procedure bestaat uit drie fases:

* De crisis analyseren, isoleren en herstellen.
* Opvolgen van de situatie.
* Post-Crisis Review.

Tijdens de eerste meeting van het Crisis Management Team worden de analyse en evaluatie van de crisissituatie samen met de eerste acties om de crisis te isoleren en herstellen besproken. De volgende meetings focussen voornamelijk op de opvolging van de situatie.

Wanneer het crisismanagement plan gedeactiveerd wordt, moet een post-crisis review uitgevoerd worden door het Crisis Management Team.

## 3.1. Een Crisis analyseren, isoleren en herstellen

Om de impact van een crisissituatie te kunnen analyseren en evalueren, zal het Crisis Management Team de volgende acties ondernemen:

| Stap/ Actie | Wie is bevoegd? | Verwijzing naar bijhorende documenten |
| --- | --- | --- |
| [Omschrijving van actie]  | [Functieomschrijving van wie bevoegd is om de actie uit te voeren] | [Bijhorende documenten] |
| Een snelle analyse maken van de situatie, gebaseerd op beschikbare informatie. | Crisis Manager |  |
| Samenstelling van het CMT. | Crisis Manager of afgevaardigden |  |
| Uitnodigen van CMT-leden (specifieer locatie indien nodig)/ zet call op met CMT-leden[[1]](#footnote-1). | Crisis Manager of afgevaardigden of Secretaris/-esse |  |
| Houden van eerste vergadering van het CMT. | CMT | Agenda voor de eerste meeting van het CMT ‘zie bijlage VII, 7.3). |
| … |  |  |

## 3.2. Deactivatie en post-crisis review

De Crisis Manager beslist wanneer geen verdere CMT-meetings meer nodig zijn om de situatie aan te pakken. Hierna keren alle afdelingen terug naar *business as usual*. De beslissing om het CMP formeel te beëindigen moet officieel vastgelegd worden.

De volgende acties worden genomen:

| Stap/ Actie | Wie is bevoegd? | Verwijzing naar bijhorende documenten |
| --- | --- | --- |
| [Omschrijving van actie]  | [Functieomschrijving van wie bevoegd is om de actie uit te voeren] | [Bijhorende documenten] |
| Communiceer naar alle belanghebbenden (intern en extern). | Crisis Manager of afgevaardigden |  |
| Bepalen wie de leiding heeft voor opvolgingsvragen. | Crisis Manager |  |
| Moment vastleggen voor post-incident review en vastleggen welke elementen hiervoor verzameld moeten worden. | Secretaris/-esse |  |
| … |  |  |

Wanneer een crisissituatie beëindigd wordt, moet een post-crisis review uitgevoerd worden, inclusief het bepalen van post-crisis actiepunten. (zie template post-incident review)

Hoofdstuk IV
CMT-meeting locaties

## 4.1. Conference calls

Conference calls tijdens crisissituaties kunnen worden gehouden via:

**<Noteer telefoonnummer of relevante contactinformatie>**

## 4.2. Hoofdlocatie

**Indien** **[adres] beschikbaar en operationeel is**, worden deze locaties gebruikt voor het crisis management:

| Functie | Locatie | Naam |
| --- | --- | --- |
| CMT-vergaderruimte. | [Adres locatie] | [Naam locatie] |
| Break out meeting rooms. | [Adres locatie] | [Naam locatie] |
| … |  |  |
|  |  |  |

## 4.3. Backup locaties

Indien de hoofdlocatie NIET operationeel en beschikbaar is, (in geval van evacuatie of schade aan het gebouw), zullen de volgende locaties -in volgorde- gebruikt worden, eventueel ter aanvulling van conference calls:

### 4.3.1 – locatie [A]

| Functie | Locatie | Naam |
| --- | --- | --- |
| CMT-vergaderruimte. | [Adres locatie] | [Naam locatie] |
| Break out meeting rooms. | [Adres locatie] | [Naam locatie] |
| … |  |  |
|  |  |  |

### 4.3.2 – locatie [B]

| Functie | Locatie | Naam |
| --- | --- | --- |
| CMT-vergaderruimte. | [Adres locatie] | [Naam locatie] |
| Break out meeting rooms. | [Adres locatie] | [Naam locatie] |
| … |  |  |
|  |  |  |

Hoofdstuk V
Goedgekeurde manieren van communiceren

De volgende manieren van communiceren zijn beschikbaar en goedgekeurd:

* Fysieke locaties (zie punt 7).
* Conference calls (zie punt 7).
* Persoonlijke mobiele telefoons voor 1-1 of groepscommunicatie *(indien relevant, hier guideline over het opzetten van groepscalls toevoegen).*
* Extra sim-cards uitgereikt aan **[…]**.
* Messaging tools (bv. Threema).
* E-mail.
* Back-up telefoons beschikbaar bij **[…]**.
* **[…]**.

Zie appendix 1 voor een lijst met contactgegevens voor noodgevallen.

**[Functie]** in het Crisis Management Team is verantwoordelijk voor de coördinatie van de communicatie en het opvolgen van eventuele problemen.

Hoofdstuk VI
Cruciale data

De cruciale data bevatten essentiële informatie en moeten snel beschikbaar zijn in crisissituaties. Onderstaande lijsten worden als cruciale data beschouwd:

* Locaties van assets.
* Overzicht en locatie van relevante plannen (bv. Incident Response Plan, Business Continuity Plan, …).
* Voorbereide verklaringen en andere communicatieboodschappen.
* …

## 6.1. Locaties van activa

Deze lijst bevat een overzicht van de locatie van alle relevante assets van **[naam bedrijf]** in crisissituaties:

| Asset | Beschrijving | Locatie |
| --- | --- | --- |
| [Naam asset] | [Waarom is dit relevant?] | [Fysieke of online locatie] |
|  |  |  |
|  |  |  |
|  |  |  |

## 6.2. Overzicht en locatie van relevante plannen

Onderstaande lijst geeft een overzicht van de locatie van de voor [Naam bedrijf] belangrijke documenten in geval van crisissituaties:

| Plan | Beschrijving | Locatie |
| --- | --- | --- |
| [Naam plan] | [Waarom is dit relevant?] | [Fysieke of online locatie] |
| bv. incident response plan. | Bevat incident response procedure. | P-drive\... |
| … |  |  |
|  |  |  |

## 6.3. Voorbereide verklaringen en communicatieboodschappen

Onderstaande verklaringen worden ter beschikking gesteld voor communicatiedoeleinden:

| Verklaring | Inhoud |
| --- | --- |
| [Verklaring] | [Inhoud] |
| bv. crisis vastgesteld. | Een incident is geëscaleerd tot een crisis op het gebied van ... |
| bv. plan geactiveerd. | Het crisisplan is geactiveerd omwille van een incident in […]. Werknemers wordt aangeraden om … |
| bv. beschadiging van uitrusting en infrastructuur. | Informeer de relevante doelgroep dat uitrusting en infrastructuur beschadigd zijn en wat de consequenties hiervan zijn op korte en lange termijn.  |
| bv. belangrijk personeel onbeschikbaar (verdwijning, kidnapping, …). | Feitelijke verklaring over belangrijk personeel (individu of groep) dat afwezig is en die verzekert dat verantwoordelijkheden en activiteiten op korte termijn zullen worden herverdeeld om de impact te beperken en dat alles gedaan wordt om de situatie aan te pakken.  |
| bv. overbelasting van netwerken/ probleem met dienstverlening. | Verontschuldiging en vraag om gedrag aan te passen om de impact te verkleinen. |
| bv. cyber-incident/ datalek. | Onderzoek loopt, situatie is opnieuw veilig of wordt opnieuw beveiligd, geef aan wat klanten/ gebruikers moeten doen ingeval dat ze impact ondervinden van de situatie, geef aan hoe ze zichzelf kunnen beschermen. |
| … |  |

Hoofdstuk VII
Bijlagen

## 7.1. Bijlage 1 – contactgegevens noodgevallen

*Noteer hier ook eventuele extra SIM-kaarten.*

### 7.1.1. Crisis Management Team

| Rol | Naam | Functie | Contactgegevens (telefoon/ mail) | Locatie |
| --- | --- | --- | --- | --- |
| [Rol] | [Naam] | [Functie] | [Contactgegevens] | [Stad, Straat, Land] |
| CEO |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Crisis Manager |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Communicatieadviseur |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| HR-verantwoordelijke |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Facilitair adviseur |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Bedrijfsjurist |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Risk & Security verantwoordelijke |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Verbindingsofficier met overheid/ regulator |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |
| Secretaris/-esse |  |  |  |  |
| [Afgevaardigde] |  |  |  |  |

### 7.1.2. Andere (overheid, leveranciers, handelaars, …)

| Rol | Naam | Contactgegevens (telefoon/ mail) | Locatie |
| --- | --- | --- | --- |
| [Rol] | [Naam] | [Contactgegevens] | [Stad, Straat, Land] |
| … |  |  |  |

## 7.2. Bijlage 2 – bijhorende documenten

* Business Impact Analysis.
* Incident Response Plan.
* Communication statements.
* …

## 7.3 Agenda van de eerste vergadering van de CMT

De agenda van de eerste vergadering van de CMT bestaat ten minste uit de volgende elementen:

| **Actie** | **Voltooid?✓ / ✕** | **Tijdstempel** |
| --- | --- | --- |
| **Opening** |  |  |
| Opening van de vergadering door de crisismanager. | [✓ / ✕] | [Tijdstempel] |
| Samenvatting van de situatie en beschikbare informatie. |  |  |
| Toewijzing van de in de CMP gedefinieerde rollen. |  |  |
| **Informatie en beoordeling** |  |  |
| Beoordeel ontbrekende informatie en ontbrekende belanghebbenden. |  |  |
| Informeer relevante belanghebbenden en geef hen de opdracht om ontbrekende informatie te verzamelen. |  |  |
| High-level beoordeling van de schade aan of de onbeschikbaarheid van:* Mensen
* Infrastructuur
* Technologie
* Informatie
* Derden

(Zie Risk Assessment) |  |  |
| Beoordeling van de evolutie van het incident: hoe zal de situatie evolueren? Is het waarschijnlijk dat de situatie zal escaleren? Wat kan er misgaan? Enz. |  |  |
| **Beveiliging en veiligheid** |  |  |
| Beoordeling van verwondingen bij mensen. |  |  |
| Beoordeling van bestaande en potentiële gevaarlijke situaties. |  |  |
| Beoordeling van de beveiliging en veiligheid van andere betrokken partijen. |  |  |
| Beslissing over en uitvoering van dringende beveiligings- en veiligheidsacties (evacuatie van het terrein, contact opnemen met de hulpdiensten, enz.). |  |  |
| Beslissing over andere acties (mededeling van algemene instructies aan het personeel in het getroffen gebied, enz.) |  |  |
| **Gevolgen voor de dienstverlening** |  |  |
| Beoordeling van de impact op de dienstverlening (huidige impact, impact tijdens de volgende piek, impact in de komende dagen, enz.) |  |  |
| Evaluatie van eventueel te activeren Business Continuity Plan (BCP). Contact opnemen met de overeenkomstige beheerder van het BCP. |  |  |
| Samenwerking met derden om de impact van de crisis waar mogelijk te beperken. |  |  |
| **Reputatie-effecten** |  |  |
| Leg de feedback van de belangrijkste externe belanghebbenden vast. |  |  |
| Evaluatie of een intensievere mediamonitoring nodig is. |  |  |
| Beoordeel specifieke acties om de impact op de reputatie te beperken. |  |  |
| **Communicatie** |  |  |
| Beslissing over de communicatie naar het personeel toe |  |  |
| Beslissing over de communicatie naar externen en/of media toe |  |  |
| **Next steps** |  |  |
| Beoordeel of er eventueel andere acties ondernomen moeten worden |  |  |
| Planning van uit te voeren taken op basis van de beschikbare middelen. |  |  |
| Documentatie van geplande acties in een logboek.  |  |  |
| Planning van de volgende vergadering |  |  |
| **…** |  |  |
| … |  |  |

1. Specifieke plannen moeten voorzien worden voor situaties waarin de gebruikelijke manieren van communiceren verstoord zijn, bv.:

Veilige communicatie kan niet gegarandeerd worden omwille van een cyberaanval.

Omwille van zware belasting in specifieke regio’s zijn bepaalde diensten niet beschikbaar of moeten beperkt worden in gebruik.

Belangrijke communicatietools zijn onbeschikbaar.

Belangrijk personeel of ondersteunende diensten zijn onbeschikbaar, waardoor de dienstverlening wegvalt of een incident minder snel kan worden opgelost. [↑](#footnote-ref-1)