Bedrijfscontinuïteitsplan <naam bevoegd gezag>

Versienummer: <xxx>

<Maand en jaartal>

Dit template is zorgvuldig samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie Creative Commons Naamsvermelding 4.0 Nederland.

<https://creativecommons.org/licenses/by/4.0/legalcode.nl>

Bij het samenstellen van dit template is gebruikgemaakt van de volgende bronnen:

* Algemene Vereniging Schoolleiders (2020) '[Medezeggenschap in tijden van crisis](https://avs.nl/actueel/nieuws/medezeggenschap-in-tijden-van-crisis-2/)'
* Kennisnet (2023) '[Cybersecuritycrisis: hoe bereid je je voor? Oefen met de BOB-methode](https://www.kennisnet.nl/artikel/21437/cybersecuritycrisis-hoe-bereid-je-je-voor-oefen-met-de-bob-methode-2/)'
* MBO Raad (2023) '[Business Continuïteit](https://aanpakibp.kennisnet.nl/app/uploads/NBADOC-P13-Business-Continuity-7-9-2023.docx)'
* SCIPR (2019) '[Starterskit Business Continuity Management](https://www.surf.nl/files/2019-03/Starterkit_Business_Continuity_Management.pdf)'

Gebruikswijzer van dit template Bedrijfscontinuïteitsplan

**Verwijder voor eigen gebruik van dit document deze en de voorgaande pagina.**

Deze gebruikswijzer is een toelichting voor het gebruik van dit template Bedrijfscontinuïteitsplan. Het template Bedrijfscontinuïteitsplan helpt slechts als richtlijn voor IBP’ers om te komen tot een specifiek beleid voor het eigen schoolbestuur, naast de uitleg [Bedrijfscontinuïteitsmanagement](https://aanpakibp.kennisnet.nl/bedrijfscontinuiteitsmanagement/) op de Aanpak IBP. Met de zoek-en-vervangfunctie kun je bijvoorbeeld wel snel de naam van het schoolbestuur invullen, maar daarmee is het document nog niet geschikt om aan een bestuur voor te leggen. Vaak zal IBP bovenschools geregeld worden. <naam schoolbestuur> kun je dan vervangen door de naam van de overkoepelende instelling.

Dit bedrijfscontinuïteitsplan (BCP) bestaat uit:

* een crisismanagementplan, dat beschrijft hoe de organisatie wil handelen bij een crisis;
* uitwegscenario's en uitwegplannen, die beschrijven welke alternatieven er zijn als bepaalde applicaties uitvallen, en hoe die geactiveerd moeten worden;
* een beschrijving van de manier waarop de organisatie bedrijfscontinuïteitsmanagement heeft ingericht;
* een test- en oefenplan met afspraken over jaarlijkse oefeningen.

Omdat het normenkader zich alleen op IBP richt, richt dit template zich ook alleen op IBP-gerelateerde calamiteiten. Het is breed inzetbaar, of het nu gaat om een computernetwerk dat onbeschikbaar is, een datalek van leerlinggegevens of een ransomwareaanval op een leverancier. Hoewel de inhoud IBP-specifiek is, is de werkwijze ook geschikt te maken voor andere typen calamiteiten.

Begin met het lezen van de uitleg [Bedrijfcontinuïteitsmanagement](https://aanpakibp.kennisnet.nl/bedrijfscontinuiteitsmanagement/) op de Aanpak IBP, en pas op basis van die werkwijze dit template aan naar de situatie in jouw organisatie.

Het template gaat uit van één BCP, dat door het bevoegd gezag vastgesteld wordt voor alle scholen waarvoor het verantwoordelijk is. In de beschreven processen gaat het template uit van een relatief klein bevoegd gezag, met slechts enkele scholen onder zich. De invulling van het beleid kan per schoolbestuur op onderdelen verschillen. Van invloed kunnen zijn:

* Grootte van het schoolbestuur (bijvoorbeeld niet voldoende personen om alle taken en rollen zuiver te scheiden).
* De politieke werkelijkheid binnen een schoolbestuur (een organisatieverandering is niet altijd wenselijk, of niet op dit moment; of er is een specifieke mandatenregeling die bepaalde verantwoordelijkheden anders belegt).
* Volwassenheid van IBP in het schoolbestuur (het beleid is bijvoorbeeld te veelomvattend als onderliggende taken, rollen en functies nog niet zijn ingevuld en niet snel kunnen worden ingevuld).
* Een schoolbestuur heeft meer of minder onderliggende documenten beschikbaar om aan te refereren.
* Vormgevingseisen.

Het schoolbestuur kan afhankelijk van bovenstaande situaties kiezen om:

* Elementen weg te laten (als er bijvoorbeeld geen procesmanager is, of geen CSIRT).
* Elementen naar een bijlage te verplaatsen of enkel te refereren aan een onderliggend document, of juist in plaats van een bijlage tekst in het hoofddocument op te nemen.
* Elementen verder uit te schrijven omdat er geen onderliggende documenten zijn.

Specifiek maken van dit document

|  |  |
| --- | --- |
| <tekst> | Vervang dit door tekst die passend is bij de eigen situatie, bijvoorbeeld <naam schoolbestuur> wordt ‘Schoolbestuur X’. |
|  |  |

# Bedrijfscontinuïteitsplan <naam bevoegd gezag>

## 

## Documentgeschiedenis

### Revisies

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Auteur | Review |
| **0.1** | 1 jan 2024 | <Voornaam Achternaam> | Eerste concept uitgewerkt |
|  |  |  |  |
|  |  |  |  |

### Goedkeuring

Vastgesteld door <naam schoolbestuur>, hierna te noemen “de school”

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Functie | Versie | Datum |
| <Het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> | <Het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> |  |  |

### Documentclassificatie

|  |  |
| --- | --- |
| Classificatie | Beschrijving |
| **Openbaar** | Dit document mag zonder beperkingen worden gedeeld |
| **Vertrouwelijk** | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur> (en evt. organisaties X,Y,Z) |
| **Geheim** | Dit document is exclusief bestemd voor de volgende personen: (bijv. leden MT) |

Inhoudsopgave

[Bedrijfscontinuïteitsplan <naam bevoegd gezag> 1](#_Toc158735652)

[Documentgeschiedenis 1](#_Toc158735653)

[Revisies 1](#_Toc158735654)

[Goedkeuring 1](#_Toc158735655)

[Documentclassificatie 1](#_Toc158735656)

[Crisismanagementplan 3](#_Toc158735657)

[Activering en escalatie 3](#_Toc158735658)

[Rollen en verantwoordelijkheden 3](#_Toc158735659)

[Werkwijze 5](#_Toc158735660)

[Communicatieplan 5](#_Toc158735661)

[Aanwijzingen voor speciale noodsituaties 6](#_Toc158735662)

[Contactenlijst voor relevante externe partijen 7](#_Toc158735663)

[Uitwegscenario's en bijbehorende uitwegplannen 8](#_Toc158735664)

[Scenario 1: Belangrijke applicatie is onbeschikbaar (voorbeeld) 8](#_Toc158735665)

[Beschrijving van de BCM-organisatie 8](#_Toc158735666)

[Toewijzen van rollen 8](#_Toc158735667)

[Beheer van het BCP (dit document) 9](#_Toc158735668)

[Test- en oefenplan 9](#_Toc158735669)

## Crisismanagementplan

### Activering en escalatie

Als zich een calamiteit voordoet, zal de organisatie deze in eerste instantie proberen op te lossen binnen de normale rollen en verantwoordelijkheden. Voor kleinere incidenten zal dit voldoende zijn. Bekijk voor meer details de [uitleg Incidentmanagement](https://aanpakibp.kennisnet.nl/incidentmanagement/) op de Aanpak IBP.

Is een calamiteit niet meer binnen de normale rollen en verantwoordelijkheden op te lossen, dan spreken we van een crisis. In dat geval activeert de organisatie de crisismanagementstructuur, zodat het beheersen van de crisis centraal belegd wordt bij een crisismanagementteam (CMT). Het normale gezag geeft hun het mandaat om maatregelen te treffen om de crisis te beheersen.

Er zijn twee niveaus van escalatie: oranje en rood.

Bij escalatieniveau *oranje* is er een calamiteit die versnelde besluitvorming, directe bestuurlijke aandacht of een vergrote inzet vereist. De crisis blijft beperkt tot één school, en eventuele media-aandacht is alleen lokaal. Er wordt een lokaal CMT geactiveerd, dat wordt voorgezeten door de schoolleider.

* Het besluit over escalatieniveau oranje wordt genomen door de schoolleider, op voordracht van een teamleider van een van de betrokken teams van de school.
* De schoolleider informeert het bevoegd gezag en de teamleiders van de school over het instellen van een CMT.
* <Voeg hier eventueel meer criteria, stappen of informatielijnen toe, afhankelijk van jullie situatie>

Escalatieniveau *rood* is het hoogste niveau. Er is sprake van een crisis die schooloverstijgend is, die nationale media-aandacht krijgt, of die complexe afstemming met meerdere partners vereist. Er wordt een centraal CMT geactiveerd, dat wordt voorgezeten door het bevoegd gezag. Op elke betrokken school wordt een locatieteam ingericht, dat met het centrale CMT afstemt.

* Het besluit over escalatieniveau rood wordt genomen door het bevoegd gezag, op voordracht van een schoolleider of de teamleider van een van de betrokken teams van het bevoegd gezag.
* Het bevoegd gezag informeert de schoolleiders en de teamleiders van het bevoegd gezag over het instellen van een CMT.
* Het bevoegd gezag instrueert betrokken schoolleiders om een locatieteam in te richten, dat met het centrale CMT afstemt. De schoolleider beslist over de samenstelling van dit locatieteam, zodat het aansluit op de aard en omvang van de crisis.
* <Voeg hier eventueel meer criteria, stappen of informatielijnen toe, afhankelijk van jullie situatie>

### Rollen en verantwoordelijkheden

Het CMT is verantwoordelijk voor de beheersing van de crisis, door:

* het onder controle brengen van de crisis;
* het nemen van maatregelen om de primaire processen zoveel mogelijk te laten doorgaan of te herstellen;
* het aanbieden van adequate zorg zoals begeleiding bij traumaverwerking;
* het verzorgen van interne en externe communicatie;
* het verlenen van alle door bevoegde instanties of hulpverleners verlangde medewerking;
* het bijhouden van een logboek.

Deze opsomming is overgenomen uit het [voorbeelddocument Business Continuity](https://aanpakibp.kennisnet.nl/app/uploads/NBADOC-P13-Business-Continuity-7-9-2023.docx) van MBO Digitaal.

Na de crisis is het CMT verantwoordelijk voor de evaluatie van de crisisbeheersing. Het formuleert de te nemen preventieve maatregelen ter voorkoming van een dergelijke gebeurtenis in de toekomst. De voorzitter neemt hiertoe het initiatief en is verantwoordelijk voor uitvoering van de evaluatie.

Het CMT kent de volgende rollen:

* voorzitter: zit de vergaderingen voor
  + te vervullen door: schoolleider (bij oranje) of bestuurder (bij rood)
  + achtervang: <persoon/functie>
* secretaris: schrijft notulen en besluitenlijsten
  + te vervullen door: <persoon/functie>
  + achtervang: <persoon/functie>
* informatiecoördinator: verzamelt en presenteert het informatiebeeld
  + te vervullen door: <persoon/functie>
  + achtervang: <persoon/functie>
* inhoudelijk expert (naar behoefte): adviseert vanuit eigen expertise
  + te vervullen door: <persoon/functie>
  + achtervang: <persoon/functie>
* expert communicatie: adviseert over communicatieaspecten
  + te vervullen door: <persoon/functie>
  + achtervang: <persoon/functie>
* observator/evaluator: noteert observaties over het verloop van de crisisbeheersing en bereidt evaluatie voor
  + te vervullen door: <persoon/functie>
  + achtervang: <persoon/functie>

De voorzitter kan ervoor kiezen enkele van deze rollen samen te voegen, of juist rollen toe te voegen als de aard van de crisis daarom vraagt.

Het logboek van het CMT bevat alle relevante informatie om achteraf na te gaan hoe de crisisbeheersing is verlopen. Het vormt daarmee een aanvulling op vastlegging in het reguliere incidentmanagementproces. De secretaris houdt het logboek bij. Het logboek bestaat uit:

* de notulen van het CMT, inclusief besluitenlijst;
* vastlegging van alle schriftelijke communicatie door het CMT, inclusief tijdstip, kanaal en doelgroep;
* een overzicht van getroffen noodvoorzieningen, inclusief tijdstip van inzet.

De bedrijfshulpverleningsorganisatie (BHV) heeft ook een rol bij een crisis. <Vul hier in hoe de afstemming en samenwerking tussen het CMT en de BHV-organisatie er binnen jullie organisatie uit zal zien.>

### Werkwijze

Het CMT overlegt zo vaak als de voorzitter nodig vindt. Aan het begin van een crisis zal dit vaker zijn. Naarmate een crisis langer duurt, en er minder ontwikkelingen zijn, kan er meer tijd tussen de overleggen zitten.

In de overleggen maakt het CMT gebruik van de BOB-methode. Met deze methode kan een crisisoverleg efficiënt en effectief verlopen, waarbij de belangrijkste zaken aan bod komen.

BOB staat voor Beeldvorming, Oordeelsvorming, Besluitvorming. Een overleg dat met de BOB-methode werkt, begint met de beeldvorming. Alle deelnemers brengen feitelijke informatie in waarover zij beschikken. Deze informatie wordt nog niet geduid. Op basis van deze feitelijke informatie identificeert de voorzitter relevante thema's om te bespreken en over te besluiten. Deze vormen de agenda voor de rest van het overleg.

De thema's worden nu een voor een besproken. Bij elk thema vindt eerst oordeelsvorming plaats, direct gevolgd door besluitvorming. Oordeelsvorming gaat over wat we verwachten op basis van de feiten, welke scenario's waarschijnlijk zijn, en wat we proberen te bereiken. Besluitvorming bestaat uit het concretiseren van de volgende stappen: wat besluiten we te doen, wie is daarvoor verantwoordelijk, en wanneer verwachten we dat het klaar is?

De vergadering eindigt met het herhalen van de besluiten, en een afspraak wanneer het CMT weer bij elkaar komt.

Een [uitgebreidere uitleg](https://www.kennisnet.nl/artikel/21437/cybersecuritycrisis-hoe-bereid-je-je-voor-oefen-met-de-bob-methode-2/) over de BOB-methode is te vinden op de website van Kennisnet.

### Communicatieplan

<Als jouw bevoegd gezag al een communicatieplan heeft, zorg dan dat de tekst in deze paragraaf aansluit bij dat plan. Je kunt vanaf hier ook naar dat plan verwijzen.>

Het CMT is verantwoordelijk voor de interne en externe communicatie ten tijde van een crisis. Denk hierbij aan persvragen en contact met leveranciers en autoriteiten, maar ook aan het informeren van ouders, leerlingen en medewerkers.

Leg alle schriftelijke communicatie vast in het logboek van het CMT.

#### Mediarichtlijnen

Een crisis kan gepaard gaan met veel media-aandacht. Dat is op zich niet erg: berichten in de media kunnen helpen om mensen op de hoogte te houden van de ontwikkelingen. Maar het is wel belangrijk om zorgvuldig te zijn in het contact met de media.

* Media-contact over een crisis verloopt altijd via een vaste contactpersoon: de woordvoerder of communicatieadviseur.
* Andere medewerkers verwijzen journalisten met vragen naar deze contactpersoon.
* Wees in contact met de media altijd feitelijk, en gericht op de boodschap die wat jullie betreft centraal moet staan.
* Vermijd speculatie, in het bijzonder als het gaat over bredere impact dan de eigen organisatie.
* Vermijd schuldvragen, in het bijzonder wanneer de crisis nog in volle gang is.

#### Veelgestelde vragen

Vragen vanuit de media:

* Wat is er precies gebeurd: wie is betrokken, wat is er gebeurd, waar, wanneer, hoe?
* Hoe ernstig is de situatie?
* Wat kan er nog meer gebeuren?
* Hoe heeft dit kunnen gebeuren?
* Wat is er misgelopen?
* Wie is schuldig?
* Neemt de organisatie deze feiten serieus?
* Wat gaat er nu gebeuren?
* Wat ga je ondernemen om dit in de toekomst te voorkomen? Welke maatregelen zijn er al getroffen of gepland?
* Wanneer krijgen we nieuwe informatie en via welk kanaal?

Vragen vanuit medewerkers:

* Wat betekent deze crisis voor mij als werknemer?
* Wat moet ik ondernemen als medewerker? Welke richtlijnen moet ik volgen?
* Waar kan ik hulp vinden (bv. psychosociale ondersteuning)?
* Wat gaat de organisatie ondernemen om de medewerkers te (blijven) ondersteunen?
* Wanneer en hoe worden wij verder geïnformeerd over deze zaak?
* Waar kan ik meer informatie vinden?
* Tot wie kan ik me richten met vragen?

Vragen vanuit ouders en leerlingen:

* Wie zijn er door deze calamiteit getroffen?
* Wat betekent dit voor het onderwijs in de komende periode?
* Wat betekent dit voor toetsen en examens in de komende periode?
* Wat kunnen of moeten we thuis doen om hiermee om te gaan?
* Waar kan ik hulp vinden (bv. psychosociale ondersteuning)?
* Wanneer en hoe worden wij verder geïnformeerd over deze zaak?
* Waar kan ik meer informatie vinden?
* Tot wie kan ik me richten met vragen?

Deze lijsten zijn gebaseerd op de lijsten in het [voorbeelddocument Business Continuity](https://aanpakibp.kennisnet.nl/app/uploads/NBADOC-P13-Business-Continuity-7-9-2023.docx) van MBO Digitaal.

#### Medezeggenschap

De medezeggenschap van een school kan ook een rol spelen in de beheersing van een crisis. Welke rol dat is, hangt af van de duur van de crisis en de aard van de getroffen maatregelen.

De Wet medezeggenschap op scholen (WMS) schrijft voor in welke gevallen het nodig is de (G)MR te raadplegen. Voor noodmaatregelen is dat meestal niet (vooraf) nodig is, maar voor nieuw beleid vaak wel. In de praktijk betekent dit dat naarmate een crisis langer duurt, het belangrijker wordt om de (G)MR te betrekken bij de crisisbeheersing.

Zie voor meer informatie ook [dit artikel](https://avs.nl/actueel/nieuws/medezeggenschap-in-tijden-van-crisis-2/) van de Algemene Vereniging Schoolleiders.

<Vul hier aan op welke manier het CMT deze afweging maakt, en hoe het de (G)MR zal betrekken tijdens een crisis.>

### Aanwijzingen voor speciale noodsituaties

De Aanpak IBP bevat meerdere stappenplannen om op te treden in specifieke noodsituaties:

* [Ransomware](https://aanpakibp.kennisnet.nl/ransomware/)
* [DDoS-aanvallen](https://aanpakibp.kennisnet.nl/ddos-aanvallen/)
* [Phishingaanvallen](https://aanpakibp.kennisnet.nl/phishing/)

### Contactenlijst voor relevante externe partijen

<Deze paragraaf is sterk IBP-specifiek. Wil je dit plan ook voor andere calamiteiten gebruiken, dan zul je meer categorieën moeten toevoegen.>

#### Ict-leveranciers

<Vul hier de contactgegevens van je belangrijkste leveranciers in. Dat zijn in elk geval alle leveranciers van de systemen die terugkomen in de uitwegplannen in het volgende hoofdstuk. Als je een vaste leverancier hebt voor incidentresponsdiensten bij cybersecurityincidenten, neem die dan ook op.>

##### Leverancier 1 (voorbeeld)

* Contactpersoon regulier:
  + Telefoon:
  + E-mail:
* Contactpunt 24/7: (indien van toepassing)
  + Telefoon:
  + E-mail:

#### CERT voor het funderend onderwijs

Het Computer Emergency Response Team voor het funderend onderwijs is onderdeel van Kennisnet. Het is te bereiken via het support-team. Zie voor contactgegevens <https://www.kennisnet.nl/contact/>.

* Bereikbaarheid: 8u-17u ma t/m vr, niet op feestdagen

<Deze informatie wordt in de komende maanden bijgewerkt.>

#### Gemeentes

<Neem hier voor elke gemeente waarin je scholen gevestigd zijn, relevante contactinformatie op. Dit zal gaan om mensen bij wie je calamiteiten moet melden, perswoordvoerders en eventuele anderen.>

#### Politie

<Neem hier contactgegevens op van lokale relevante politieteams. Dat zijn degenen bij wie je aangifte moet doen van een hack.>

#### PO-Raad/VO-raad perswoordvoerder

De contactgegevens van de perswoordvoerders van de PO-Raad en VO-raad vind je hier:

* PO-Raad: <https://www.poraad.nl/contact>
* VO-raad: <https://www.vo-raad.nl/pers>

#### Onderwijsinspectie

Een IBP-gerelateerde calamiteit kun je bij de Onderwijsinspectie melden via <https://contactformulier.onderwijsinspectie.nl/contact>.

Onregelmatigheden rond de examens moeten worden doorgegeven via het [Examenloket](https://duo.nl/zakelijk/voortgezet-onderwijs/examens-en-diplomas/examenloket/).

#### Autoriteit Persoonsgegevens

Betreft de calamiteit ook een datalek, dan kun je dat bij de Autoriteit Persoonsgegevens melden via [hun website](https://autoriteitpersoonsgegevens.nl/datalek-melden). In sommige gevallen ben je daartoe [verplicht](https://aanpakibp.kennisnet.nl/beveiligingsincidenten-en-datalekken-melden/).

## Uitwegscenario's en bijbehorende uitwegplannen

Om het CMT te ondersteunen heeft het bevoegd gezag voor de belangrijkste applicaties uitwegplannen opgesteld. Zo kunnen kritische bedrijfsprocessen zo goed mogelijk doorgaan.

<In dit hoofdstuk leg je de resultaten van de workshop vast die je georganiseerd hebt op basis van de handreiking Aanpak BCM. We geven hier een voorbeeld. Voeg zelf per scenario alle relevante uitwegplannen in.>

### Scenario 1: Belangrijke applicatie is onbeschikbaar (voorbeeld)

*Als er sprake is van een verstoring van ’belangrijke applicatie’, is het niet mogelijk om op de gewone manier les te geven. Het CMT kan dan gebruikmaken van de volgende uitwegplannen.*

*Elke activering van een uitwegplan moet worden vastgelegd in het logboek.*

#### Uitwegplan 1: Alternatieve applicatie (voorbeeld)

*Omschrijving: In plaats van belangrijke applicatie, kan er ook tijdelijk gebruikgemaakt worden van alternatieve applicatie. Alternatieve applicatie beschikt over de meeste functionaliteit van belangrijke applicatie, maar werkt niet in <geval 1>, <geval 2> en <geval 3>.*

*Voor het activeren van alternatieve applicatie:*

*\* Beschrijf wie er wat doet om dit uitwegplan te activeren.*

*\* Beschrijf ook benodigde contacten met externe partijen, zoals leveranciers.*

*\* Beschrijf wie er moet worden geïnformeerd, of van wie er akkoord nodig is.*

*\* Beschrijf hoe de relevante informatie bij betrokkenen terechtkomt.*

#### Uitwegplan 2: Analoog alternatief (voorbeeld)

*Omschrijving: Als belangrijke applicatie niet beschikbaar is, kunnen we ook overstappen naar analoog alternatief. Analoog alternatief kan alleen in beperkte mate de functionaliteit van belangrijke applicatie bieden, namelijk <functionaliteit 1>.*

*Voor het activeren van analoog alternatief:*

* *enzovoort.*

## Beschrijving van de BCM-organisatie

De BCM-organisatie is ingericht in lijn met de [uitleg BCM](https://aanpakibp.kennisnet.nl/bedrijfscontinuiteitsmanagement/). Dit hoofdstuk werkt dit verder uit en beschrijft waar we van de handreiking afwijken.

### Toewijzen van rollen

In onze organisatie zijn er BCM-rollen in de koude fase (geen escalatie) en de warme fase (escalatie naar oranje of rood, inrichting CMT).

In de koude fase bestaat de BCM-organisatie uit één functionaris:

* De BCM-coördinator: degene die de processen rond BCM uitvoert, zoals het initiëren van een jaarlijkse oefening en update van het bedrijfscontinuïteitsplan.
  + Onze BCM-coördinator is: <vul naam in, bijvoorbeeld de IBP-verantwoordelijke die dit onderwerp aanjaagt>

In de warme fase gaat het om de leden van het CMT en locatieteams bij de betrokken scholen. Zie de paragraaf ‘Activering en escalatie’ voor een lijst. De BCM-coördinator heeft geen rol tijdens de warme fase. Deze persoon kan daarnaast natuurlijk wel een andere rol vervullen.

Alle mensen die gevraagd kunnen worden voor een CMT of een locatieteam, worden vooraf op de hoogte gesteld van hun rol. Ook krijgen ze de benodigde instructie. <Vul hier aan hoe dat er concreet in jullie organisatie uit zal zien.>

### Beheer van het BCP (dit document)

Dit document wordt jaarlijks bijgewerkt, zoals beschreven in de [uitleg BCM](https://aanpakibp.kennisnet.nl/bedrijfscontinuiteitsmanagement/). Bij deze update worden nieuwe maatregelen en uitwegplannen vastgelegd. Ook vindt er een check plaats op de lijst met contactgegevens, zodat die up-to-date blijft. Na elke wijziging wordt het plan aan het bevoegd gezag voorgelegd voor akkoord.

Als de structuur van de organisatie verandert, bijvoorbeeld bij een fusie, worden ook de BCP's van de organisaties samengevoegd. In eerste instantie zal de ict nog niet geïntegreerd zijn, en bestaan ook meerdere uitwegplannen dus naast elkaar. Naarmate de ict verder geïntegreerd wordt, kunnen deze plannen stapsgewijs vereenvoudigd worden.

## Test- en oefenplan

De BCM-coördinator organiseert elk jaar een oefening om het BCP in de praktijk te testen. Deze oefening wordt georganiseerd op basis van de adviezen uit de [uitleg BCM](https://aanpakibp.kennisnet.nl/bedrijfscontinuiteitsmanagement/).

In deze oefening stellen we een CMT samen om een fictieve crisis te beheersen. We betrekken in elk geval een of meer van de applicaties waarvoor we uitwegplannen hebben opgesteld. Zo kunnen we in de praktijk zien hoe deze plannen werken.

<Alleen als het bevoegd gezag ook it-herstelplannen heeft

Ook de it-herstelplannen voor kritische systemen moeten jaarlijks worden getest. Het gaat voor onze organisatie om de volgende systemen:

* <systeem 1>
* <systeem 2>

De manier waarop deze plannen worden geoefend, wordt in die plannen beschreven.>