

Netcentrische samenwerking

Stappenplan

25 februari 2026



Nederlands Instituut Publieke Veiligheid
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.nipv.nl
info@nipv.nl
088 274 74 00

Colofon

Ondanks de aan de samenstelling van de tekst bestede zorg kan de samensteller geen aansprakelijkheid aanvaarden voor schade ontstaan door eventuele fouten c.q. onvolkomenheden in dit document.

Om deze publicatie te kunnen blijven ontwikkelen en verbeteren, ontvangen wij graag commentaar en suggesties ter verbetering. Vragen of opmerkingen kunt u sturen naar netcentrischwerken@nipv.nl.

© Nederlands Instituut Publieke Veiligheid (NIPV), 2026

Auteur(s)	Frank Bruinink, Bregje Veldman
Opdrachtgever	Martijn van der Werff, programmamanager Landelijke Voorziening Crisisbeheersing
Datum	25 februari 2026
Status	Definitief
Versie	2.0

Wij hechten veel belang aan kennisdeling. Delen uit deze publicatie mogen dan ook worden overgenomen op voorwaarde van bronvermelding.

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

Inhoud

Inleiding	4
Leeswijzer	5
1. Verkenningsfase	5
Stap 1 – Verkennen	5
Stap 2 – Ambitie	7
2. Uitwerkingsfase	8
Stap 3 – Uitwerken project	8
Stap 4 – Implementeren	8
3. Uitvoeringsfase	13
Stap 5 – Toewerken naar Go-live moment	13
Stap 6 – Stay-live	14
Bijlagen	15
Bijlage 1: Voorbeeld Processchema in fases	15
Bijlage 2: Stappenplan aanschaf en inrichting Techniek	16
Bijlage 3: Vragenlijst 3 - Staat van Netcentrisch Werken	17

Inleiding

De samenwerking tussen een crisispartner en één of meerdere veiligheidsregio's gaat verder dan enkel een technische koppeling. Een goede samenwerking betekent dat er afspraken gemaakt worden over hoe die samenwerking er precies uit ziet. Hoe wordt informatie uitgewisseld? Met wie? Op welk moment? En om wat voor informatie moet het dan gaan? Dit document beschrijft de te doorlopen stappen om te komen tot een effectieve samenwerking tussen veiligheidsregio's en crisispartners, op basis van de netcentrische werkwijze.

Dit stappenplan is bedoeld als leidraad voor gesprekken tussen de crisispartner die de ambitie heeft om aan te sluiten op de netcentrische werkwijze in de crisisrespons, en een crisispartner die al is aangesloten en als begeleider kan optreden. Het biedt handvatten voor het scheppen van de randvoorwaarden die nodig zijn om deze samenwerking te realiseren.

Het is een praktische uitwerking van het Referentiekader Netcentrische Crisisbeheersing, waarin de Landelijke Voorziening Crisisbeheersing (LVCb), de netcentrische basisprincipes en de netcentrische doctrine worden toegelicht.

Gebruik TGV en Verkeersplein/Diginetwerk

Dit stappenplan Netcentrische samenwerking is geactualiseerd vanwege twee belangrijke ontwikkelingen:

- › de Toegangsservice Gezamenlijke Voorzieningen (TGV), die als landelijke en beveiligde toegangspoort voor onder andere het LCMS fungeert
- › de rol van het ICT-Verkeersplein en Diginetwerk als robuuste, besloten netwerkvoorzieningen voor veilige en continue samenwerking.

Deze aanvullingen ondersteunen crisispartners bij een toekomstbestendige en betrouwbare aansluiting op de netcentrische werkwijze.

De Landelijke Voorziening Crisisbeheersing (LVCb) helpt zo'n 1000 organisaties samenwerken in alle fases van crisisbeheersing. Dit gebeurt via de werkwijze 'netcentrisch werken' en een platform met veilige systemen die de besluitvorming ondersteunen. Het Landelijk Crisismanagement Systeem (LCMS) is één van die systemen.

Crisispartners staan via de LVCb met elkaar in verbinding, waardoor ze voor, tijdens en na de crisis rijke en actuele beelden kunnen uitwisselen. En op basis daarvan samen de juiste en voor iedereen passende besluiten nemen.

De LVCb is voortdurend in ontwikkeling om relevant en betrouwbaar te zijn en blijven voor de gebruikers. Zo integreren we data en BI om de beelden in het LCMS te verrijken. En verbeteren we de continue beschikbaarheid van het platform door aan te sluiten op het Diginetwerk. Ook de werkwijze is altijd in ontwikkeling: in samenwerking met onze academische partners sluiten we steeds aan op de nieuwste wetenschappelijke inzichten.

Leeswijzer

Het stappenplan bestaat uit drie verschillende, maar met elkaar samenhangende fases:

- > Verkennen,
- > Uitwerken,
- > Uitvoeren.

Het eerste hoofdstuk beschrijft welke stappen nodig zijn om te starten met de netcentrische samenwerking. Het tweede hoofdstuk beschrijft de producten die moeten worden uitgewerkt om vervolgens tot de uitvoering van de implementatie te kunnen komen (hoofdstuk drie).

1. Verkenningsfase

De verkenningsfase staat in het teken van het onderzoeken waarom een organisatie netcentrisch wil gaan werken en wat de meerwaarde daarvan zou kunnen zijn. Daarnaast wordt in deze fase de huidige samenwerking tussen al aangesloten crisispartners zoals veiligheidsregio('s), en de aan te sluiten crisispartner in kaart gebracht. Het uitgangspunt is hierbij steeds: welke problemen of knelpunten bestaan er in de huidige samenwerking, en dan met name de aspecten die betrekking hebben op het delen en uitwisselen van informatie.

Tegelijkertijd worden in deze fase de wederzijdse ambities uitgesproken, wordt een basis gelegd voor hoe de samenwerking er in de toekomst uit moet komen te zien, en wordt de context waarin de betrokken organisaties acteren geschetst.

Stap 1 – Verkennen

Tijdens de eerste stap wordt een verkenning gedaan naar:

- > Het bestaande informatiemanagementproces,
- > De bekendheid met de netcentrische werkwijze.
- > Het werken met het LCMS.

In deze stap wordt antwoord gegeven op de vragen: *‘Kan de netcentrische werkwijze helpen om eventueel bestaande knelpunten binnen de uitwisseling van informatie op te lossen?’*. En, *‘Zou de netcentrische wijze van informatiedelen meerwaarde kunnen geven aan de bestaande respons op crises?’*

Waarom wil een organisatie netcentrisch werken?

Allereerst wordt in kaart gebracht waarom een organisatie netcentrisch wil gaan werken. Van belang is om te achterhalen wat de vraag achter de vraag is en of de netcentrische werkwijze daar een oplossing voor biedt. In deze fase ligt de focus met name op onderzoeken of er, en zo ja welke, knelpunten er zijn ten aanzien van het uitwisselen van informatie. Vervolgens moet bepaald worden welk doel de organisatie met de netcentrische werkwijze wil bereiken en of het probleem daarmee daadwerkelijk wordt opgelost.

Als eerste stap kan bijvoorbeeld gedacht worden aan het organiseren van een nulmeting (een soort ‘table top-oefening’ waarin door middel van een casus knelpunten ‘aangeboden’ worden) waaruit naar voren komt hoe de organisatie nu samenwerkt en informatie uitwisselt; intern, maar ook

met andere organisaties. Zo ontstaat een beeld van de huidige knelpunten. Daarnaast kan uitleg gegeven worden over de netcentrische werkwijze en een demonstratie van het ondersteunende systeem LCMS. Dit om in te schatten of dit een oplossing biedt voor de geformuleerde knelpunten.

Tot slot vergt het implementeren van de netcentrische werkwijze een veranderproces. Om dit veranderproces goed te laten verlopen is het wenselijk dat er op alle niveaus commitment is en betrokkenen binnen de organisatie de ruimte krijgen om de nieuwe werkwijze te doorleven.

Betrokken partijen

Bij het implementatietraject van nieuwe partners spelen, naast de betreffende nieuwe organisatie zelf, drie organisaties een rol:

- > Het Nederlands Instituut Publieke Veiligheid (NIPV)
- > De implementatiepartner
- > De adoptiepartner

Nederlands Instituut Publieke Veiligheid

Het NIPV is vaak de eerste organisatie waar crisispartners aankloppen als ze netcentrisch willen werken met het Landelijk Crisis Management Systeem (LCMS). Het NIPV is eigenaar van de doctrine en beheerder van het systeem LCMS, en heeft daarmee een verbindende rol tussen alle crisispartners. Daarnaast bewaakt het NIPV de kwaliteit van de netcentrische werkwijze en is het verantwoordelijk voor de doorontwikkeling van zowel de werkwijze als het systeem. Vanuit de rol van kwaliteitsbewaker is het NIPV bij de start en bij de afronding Go-live betrokken bij het implementatieproces.

Implementatiepartner

Voor een succesvolle uitvoering van het implementatieproces is het essentieel om één van de door het NIPV gecertificeerde Implementatiepartners te betrekken. De praktijk wijst uit dat deze partners, die relevante ervaring meebrengen, een cruciale rol spelen in het adviseren over het plan van aanpak en het ondersteunen bij de uitvoering ervan. Ze zijn tevens verantwoordelijk voor het toelichten en uitdragen van de netcentrische werkwijze, inclusief de tien basisprincipes, en zorgen voor de inrichting van sjablonen en profielen in LCMS. Bovendien verzorgen ze (delen van) het OTO-traject. Tijdens de implementatie kan, wanneer deze wordt ondersteund door een gecertificeerde implementatiepartner, kosteloos gebruik worden gemaakt van de oefenomgeving van LCMS.

De kwaliteit van de implementatie en het netcentrisch werken is cruciaal, aangezien partners die op netcentrische wijze samenwerken volledig op elkaar moeten kunnen rekenen en duidelijk moeten weten wat ze aan elkaar hebben. Daarom is het van groot belang om een gecertificeerde implementatiepartner vroeg in het proces te betrekken, zodat deze het doel en de aanleiding van de implementatie goed begrijpt.

Meer informatie hierover is te vinden in de **factsheet 'Implementatie- en opleidingspartners'**.

Adoptiepartner

Voor organisaties is het aan te raden om één aanspreekpunt te hebben om de samenwerking mee vorm te geven. Daarnaast is het voor alle overige crisispartners prettig om geen dubbel werk te hoeven doen. Een adoptiepartner kan hierbij helpen; dit is een crisispartner die al netcentrisch werkt. In de **factsheet 'Adoptiepartner'** staat meer informatie over deze ondersteuning.

Stap 2 – Ambitie

Komt uit stap 1 naar voren dat de netcentrische werkwijze van meerwaarde kan zijn bij het oplossen van de knelpunten rondom onder andere informatie-uitwisseling? Dan kan bij stap 2 gekeken worden naar welke vorm. In deze stap wordt dus antwoord gegeven op de vraag *‘Hoe kan de netcentrische werkwijze helpen om de bestaande knelpunten binnen de uitwisseling van informatie op te lossen?’*.

Eerste inschatting en keuze van aansluitvorm

De netcentrische werkwijze is in de loop der jaren steeds breder omarmd door verschillende organisaties en is inmiddels vaak de standaard werkwijze binnen de crisisbeheersing.

Met het toetreden van steeds meer organisaties, elk met hun eigen structuren, achtergronden en rollen, ontstaan er echter diverse wensen en voorkeuren over de manier van aansluiting. Niet alle organisaties vinden het relevant of passend om hun gehele structuur volledig netcentrisch in te richten. Sommige organisaties kiezen ervoor gedeeltelijk aan te sluiten, afhankelijk van hun rol in de crisisbeheersing en hun ambities rondom netcentrisch werken. Dit kan bijvoorbeeld het geval zijn wanneer een organisatie zich in een groeifase bevindt of wanneer het om één crisisteam gaat, waarvan de leden geen vertegenwoordigers zijn van een breder samenwerkingsnetwerk. Ondanks deze verschillende benaderingen wordt in alle gevallen gesproken van een netcentrische aansluiting.

In de factsheet ‘Aansluitvormen’ wordt verder toegelicht welke verschillende manieren er zijn om aan te sluiten op de netcentrische werkwijze.

Het kan ook een conclusie zijn dat geen van de bovenstaande aansluitvormen geschikt is en dat netcentrisch samenwerken met het LCMS niet de juiste oplossing is *voor de bestaande knelpunten binnen de uitwisseling van informatie*.

2. Uitwerkingsfase

In de uitwerkingsfase worden stappen gezet om de huidige samenwerking uit te breiden en te onderzoeken wat nodig is om de netcentrische werkwijze binnen de organisatie te implementeren.

Stap 3 – Uitwerken project

In de derde stap wordt het project verder uitgewerkt door de interne projectorganisatie, met als eindresultaat een plan van aanpak van het project. Dit plan van aanpak kan ondersteunen bij het creëren van commitment bij alle betrokken functionarissen en bij het duidelijk beschrijven van de meerwaarde. Met als doel het goed doorlopen van het gehele implementatietraject.

Om dit plan uit te kunnen werken is het belangrijk een interne projectorganisatie op te richten. Daarnaast is het in deze stap essentieel om een gecertificeerde implementatiepartner te betrekken. Tot slot zijn er een aantal onderwerpen met bijbehorende vragen dat moet worden uitgewerkt:

- › Wat is het probleem dat met de netcentrische werkwijze opgelost moet worden?
- › Welke ambities en doelen zijn gesteld?
- › Aan welke kwaliteitsstandaarden willen we voldoen?
- › Hoeveel tijd en geld is er beschikbaar en hoe wordt de implementatie uitgevoerd?
- › Welke factoren kunnen van invloed zijn op de implementatie?
- › Welke functionarissen (en andere organisaties) zijn betrokken bij het implementatietraject?
- › Wat zijn de risico's en bedreigingen van het project?
- › Wat is de globale planning van het project?

Door deze vragen allemaal te beantwoorden en uit te werken wordt een inschatting gemaakt van de omvang en toegevoegde waarde van het project. Dit draagt uiteindelijk bij aan het verdere verloop van de implementatie.

Stap 4 – Implementeren

In de vierde stap wordt de blauwdruk netcentrisch werken opgesteld. Dit is een document waarin alle samenwerkingsafspraken met crisispartners en/of veiligheidsregio's worden opgenomen. In de blauwdruk zijn vier onderdelen belangrijk, namelijk: organisatie, proces, mens en techniek. Deze onderdelen vereisen een aantal acties dat in de tijd kan worden weggezet. Dit wordt hieronder verder toegelicht.

In de loop der jaren zijn door alle organisaties die wilden aansluiten op de netcentrische werkwijze blauwdrukken opgesteld. Het NIPV heeft dus een breed scala aan voorbeeldblauwdrukken die nieuwe organisaties kunnen gebruiken. Deze blauwdrukken zijn op te vragen via de adviseurs netcentrisch werken, of via netcentrischwerken@nipv.nl.

Organisatie

Bij het onderdeel 'organisatie' worden de organisatiestructuren en ambities met betrekking tot de netcentrische werkwijze beschreven. Ook wordt toegelicht hoe de informatieorganisatie eruit gaat zien en moet in kaart worden gebracht wat daarvoor nodig is. Welke mensen zijn bijvoorbeeld

nodig voor het uitvoeren van het informatiemanagementproces, en aan welke functie-eisen moeten zij dan voldoen? Hoe verhouden deze functionarissen zich tot de leden van andere crisisteams en hoe wordt georganiseerd dat alle organisatieprocessen een bijdrage leveren aan het beeld? Een organogram van de (nog te vormen) crisisorganisatie kan helpen om bovenstaande informatie inzichtelijk te maken.

Proces

Het onderdeel 'proces' heeft betrekking op vier verschillende processen die ingericht moeten worden. Deze processen vertellen uiteindelijk iets over hoe de organisatie de netcentrische werkwijze gaat toepassen.

Melding en alarmering

Het proces 'melding en alarmering' beschrijft de wijze waarop de crisisfunctionarissen worden betrokken bij een incident, crisis of ramp. Wie is hiervoor verantwoordelijk? Hoe worden zij gealarmeerd? Krijgen de functionarissen een pieper of wordt het via telefoon of een berichtendienst georganiseerd? Dat proces moet helemaal uitgeschreven worden, zodat alle betrokkenen weten hoe het in zijn werk gaat.

Op- en afschaling

In het proces 'op- en afschaling' staat beschreven wanneer de crisisorganisatie in actie komt: wanneer er op- en afgeschaald wordt, welke niveaus de organisatie hiervoor gebruikt en aan welke criteria dan moet worden voldaan.

Leiding & coördinatie

Het proces 'leiding & coördinatie' beschrijft de wijze waarop tijdens een inzet leiding wordt gegeven. Zowel bij een monodisciplinaire als een multidisciplinaire opschaling. Wie is wanneer de hoogste leidinggevende en hoe gaat het besluitvormingsproces in zijn werk? Wie maakt de keuzes? Wie geeft richting?

Informatiemanagement

Het laatste proces beschrijft hoe de verschillende informatiestromen bij elkaar komen en wie daarvoor verantwoordelijk is. Hoe wordt informatie opgehaald en verder de organisatie ingebracht, zowel intern als extern? Welke producten moet de informatieorganisatie opleveren en hoe zien deze producten eruit? Welke thema's worden bijvoorbeeld standaard gebruikt bij het opstellen van een situatiebeeld en wie moeten daarbij betrokken worden?

Mens

Bij het onderdeel mens wordt het programma van 'opleiden, trainen en oefenen' (OTO) vormgegeven en uitgevoerd. Daarin wordt onder andere beschreven wat de taken en verantwoordelijkheden van alle crisisfunctionarissen (informatiemanager, voorzitters etc.) zijn, hoe zij worden opgeleid en hoe bijvoorbeeld de tien netcentrische basisprincipes aan bod komen. Ook moet worden gekeken hoe de organisatie met alle crisisteams in samenhang de netcentrische werkwijze gaat trainen en beoefenen.

Dat vereist het opstellen van kwalificatienormen voor het werven en selecteren van crisisfunctionarissen. Het NIPV heeft voor een groot aantal crisisfunctionarissen kwalificatiedossiers opgesteld die hierbij kunnen ondersteunen, deze kwalificatiedossiers zijn [hier](#) te vinden.

Tot slot is het belangrijk dat alle crisisfunctionarissen vakbekwaam worden, maar ook na de afronding van de implementatie vakbekwaam blijven. De inrichting daarvan moet eveneens bij het onderdeel 'mens' beschreven worden.

Techniek

Als laatst worden (samenwerkings-)afspraken gemaakt over de inrichting van het ondersteunende technische systeem, het Landelijk Crisis Management Systeem (LCMS).

Dienstverleningsovereenkomst

In dit stadium wordt de dienstverleningsovereenkomst afgesloten tussen het NIPV en de crisispartner. Hierin staan wederzijdse afspraken en verplichtingen beschreven over de financiering en het gebruik van het systeem LCMS.

Gebruikersovereenkomst en organisatiebeheerders

Allereerst moet een Registratieformulier Organisatiebeheerders LCMS met daarin afspraken over beheer en controle worden ingevuld tussen het NIPV (Landelijk Functioneel Beheer) en de organisatie. Vervolgens is het belangrijk dat binnen de organisatie een aantal organisatiebeheerders wordt aangesteld. Zij krijgen vanuit het NIPV een training over deze nieuwe rol en toegang tot een SharePoint-omgeving met meer informatie over het systeem. Hoe eerder dat gedaan wordt, hoe meer profijt een organisatie daarvan heeft in de verdere inrichting van het systeem.

Inrichting systeem LCMS

Verder moet worden nagedacht over de inrichting van het systeem. Welke teams, disciplines en functies heeft de aan te sluiten organisatie nodig? Op basis van de wensen wordt dit door functioneel beheer van het NIPV ingericht, zodat de organisatie vervolgens zelf profielen aan kan maken. Ook moet worden nagedacht over het inrichten van sjablonen/templates. Alle activiteiten in het LCMS zijn opgebouwd volgens een bepaalde structuur: pagina's, velden, thema's en bullets. Deze structuur helpt organisaties bij een eenduidige werkwijze en opbouw, maar moet wel ondersteunend zijn aan de structuur van de organisatie.

Technische organisatie

Naast de te maken afspraken over het systeem LCMS, het organisatiebeheer en de in te richten organisatie in LCMS, is het ook aan te raden om na te denken over andere technische aspecten die de organisatie zelf op orde moet hebben. Denk hierbij bijvoorbeeld aan het hebben van geschikte werkplekken, ICT-voorzieningen of het beschikbaar hebben van fallback-procedures voor het geval dat de techniek niet werkt: inclusief het borgen van alternatieve netwerken en verbindingen voor het LCMS, en daarnaast de inrichting van de Toegangsservice Gezamenlijke Voorzieningen (TGV). In Bijlage 2 is een aantal van deze aspecten overzichtelijk weergegeven, met daarbij de bijbehorende actiehouders genoemd.

Toegangsservice Gezamenlijke Voorzieningen (TGV)

De toegang tot het Landelijk Crisis Management Systeem (LCMS) verloopt centraal via de Toegangsservice Gezamenlijke Voorzieningen (TGV). Gebruikers loggen dus niet rechtstreeks in op het LCMS, maar doen dit via een beveiligde toegangslaag die door het NIPV wordt beheerd.

De TGV biedt een uniforme en veilige manier van authenticatie, oftewel het vaststellen van de identiteit van een gebruiker. Daarbij blijven organisaties hun eigen accounts en aanvullende beveiligingsmaatregelen gebruiken, zoals Multi-Factor Authenticatie (MFA). Dit zorgt voor een betrouwbare én continu beschikbare toegang tot het LCMS.

Organisatorische inrichting

> TGV als centrale toegangspoort

De TGV is een landelijke toegangsservice die door het NIPV wordt beheerd. Het doel is crisis- en ketenpartners – zoals veiligheidsregio's, waterschappen, politie, Defensie en andere aangesloten organisaties – via één beveiligde omgeving toegang bieden tot gezamenlijke voorzieningen zoals het LCMS, het Veiligheidsbeeld en diverse e-learningplatforms.

> Federatieve koppeling

Partners worden aangesloten via 'federatieve authenticatie' (OIDC). Hierdoor kunnen gebruikers inloggen met hun eigen organisatieaccount, terwijl de TGV de autorisatie veilig doorgeeft aan de achterliggende applicaties. Voor organisaties die (nog) niet kunnen federeren, is een beheeromgeving beschikbaar voor gastaccounts. De Identity Provider beheerder (IdP-beheerder) van de organisatie (vaak de ICT-afdeling) speelt een centrale rol bij het inrichten van de koppeling met de TGV, en is bovendien verantwoordelijk voor het toegangsbeheer.

> Rol- en rechtenbeheer

> Gedetailleerde autorisaties, zoals rechten en profielen, worden niet in de TGV beheerd maar in het LCMS zelf. De TGV faciliteert uitsluitend de veilige toegang en biedt Single Sign-On (SSO).

Praktische stappen voor gebruikers

- > Zodra de koppeling is ingericht, gaan gebruikers via [LCMS.nl](https://lcms.nl) naar mijn.productie.lcms.nl. Daar selecteren zij hun organisatie op het TGV-inlogschermb. Vervolgens loggen zij in met hun eigen organisatieaccount.
- > Bij de eerste keer inloggen wordt een extra verificatie uitgevoerd via een eenmalige code.
- > Bij elke volgende inlogpoging is Multi-Factor Authenticatie verplicht. Hierdoor kunnen gebruikers uitsluitend inloggen met hun eigen persoonlijke account.

Netwerken en verbindingen

Veel organisaties vertrouwen op het internet voor informatie-uitwisseling met crisispartners, ook voor het gebruik van het LCMS. Maar het internet is een open netwerk dat kwetsbaar is voor storingen en cyberaanvallen. Het LCMS is daarom op twee alternatieve manieren te benaderen:

1. ICT-Verkeersplein VR

Netwerkinfrastructuur voor de veiligheidsregio's.

2. Diginetwerk

Netwerkinfrastructuur voor de overheid en organisaties met een publieke taak.

Beide netwerken hebben een besloten karakter en kunnen daardoor onafhankelijk van het open internet functioneren. Ze werken met eigen netwerkverbindingen en worden beheerd. Dit levert de volgende voordelen op:

- > Veilig: besloten netwerk, minder risico op aanvallen.
- > Efficiënt: één aansluiting voor informatie-uitwisseling met alle aangesloten organisaties.
- > Continuïteit: samenwerking blijft mogelijk, ook bij internetuitval.

Neem contact op met de adviseurs Netcentrisch werken om de mogelijkheden voor koppeling met deze netwerken te bespreken.

Afstemming met andere crisispartners

Als een nieuwe crisispartner aansluit op de netcentrische werkwijze met het ondersteunende systeem LCMS, dan sluit deze aan op een bestaand netwerk van netcentrisch werkende partijen.

Om de samenwerking tussen al deze partijen goed te laten verlopen, is een aantal kwaliteitsnormen en eisen vastgesteld, waaraan de nieuwe crisispartner dient te voldoen. Deze kwaliteitsnormen en eisen zijn opgenomen in De Staat van Netcentrisch Werken (zie stap 6).

Het is daarom van belang dat er regelmatig afstemming plaatsvindt tussen de nieuwe en al aangesloten crisispartners. Zo dient de blauwdruk bijvoorbeeld in het Netwerk Netcentrisch Werken gepresenteerd te worden, om te toetsen of aan de kwaliteitsnormen en eisen wordt voldaan. De adoptiepartner kan de crisispartner introduceren in dit netwerk, regelmatig een procesupdate geven en vragen beantwoorden.

3. Uitvoeringsfase

Tijdens de laatste fase worden alle voorbereidingen uit de eerste twee fasen in de praktijk gebracht. Deze fase bestaat uit twee stappen:

- › Toewerken naar een Go-live oefening
- › Zorgen dat de kwaliteit ook daarna wordt gewaarborgd, ook wel de Stay-livefase genoemd.

Stap 5 – Toewerken naar Go-live moment

Uitvoeren blauwdruk

Na het opstellen van de blauwdruk (stap 4) waarin de contouren van alle vier de onderdelen inclusief de uit te voeren acties staan beschreven, moet hier vervolgens concrete invulling en opvolging aan worden gegeven. Zo moeten bijvoorbeeld informatiefunctionarissen geworven worden, dienen zij opgeleid en getraind te worden en moet er geoefend worden. Ook is het belangrijk dat de techniek in het LCMS ingericht wordt volgens de gemaakte afspraken en formats, en moeten de afspraken met de regio's nageleefd worden. Door middel van het uitvoeren van alle activiteiten wordt uiteindelijk naar een gezamenlijk Go-live moment toegewerkt. In Bijlage 1 is een checklist opgenomen met de belangrijkste stappen die leiden tot een blauwdruk.

Daarnaast kan rond de Go-live worden gecontroleerd of en hoe het netcentrisch werken binnen de organisatie is geborgd. Dit kan door vragenlijst 1 uit de “Staat van Netcentrisch Werken” door te nemen, waarin de borging van Netcentrisch werken in de reguliere bedrijfsvoering wordt geëvalueerd. Neem voor meer informatie contact op met de adviseurs netcentrisch werken of via netcentrischwerken@nipv.nl

Afsluiten met go-live moment

Om de implementatieperiode succesvol af te ronden, organiseert de organisatie samen met de implementatiepartner (coördinerende partij), de adoptiepartner en in afstemming met het NIPV een Go-live oefening. Tijdens deze oefening wordt een crisis gesimuleerd waarin de netcentrische werkwijze wordt toegepast bij de bestrijding daarvan. De omvang van de oefening is afhankelijk van de aansluitvorm, maar er is een aantal criteria waaraan moet worden voldaan, dit is opgenomen in vragenlijst 3 van de Staat van Netcentrisch werken. Deze vragenlijst is als Bijlage 3 opgenomen.

Tijdens de go-live oefening zijn zowel de adoptiepartner als het NIPV aanwezig om, aan de hand van de opgestelde criteria uit de Staat van Netcentrisch Werken, te kijken hoe de organisatie de netcentrische werkwijze uitvoert. Aan het eind van de oefening wordt door het NIPV een rapportage gemaakt met daarin alle bevindingen. Hierin staan de punten die al goed gaan, samen met een aantal punten waaraan de organisatie bij de verdere invoer van de netcentrische werkwijze nog extra aandacht dient te besteden.

Na het Go-live moment krijgt de organisatie toegang tot de operationele omgeving in het LCMS, zodat deze ook tijdens een crisis of incident netcentrisch informatie met partners uit kan wisselen.

Stap 6 – Stay-live

De laatste stap van het implementatieproces is de Stay-live. Deze stap moet ervoor zorgen dat alle bovengenoemde onderdelen worden overgedragen aan de staande organisatie en dat de kwaliteit van de toepassing van de netcentrische werkwijze gewaarborgd blijft.

Staat van Netcentrisch Werken

Eén van de tools die gebruikt wordt voor het continu monitoren en evalueren van de netcentrische werkwijze met het LCMS, is de Staat van Netcentrisch Werken. Deze kwaliteitsmonitor wordt door alle netcentrisch werkende organisaties ingevuld om een beeld te genereren van de kwaliteit van deze samenwerking. In de eerste instantie genereert het een beeld van de kwaliteit van de netcentrische werkwijze binnen de betreffende sector. Bij elkaar opgeteld levert het een beeld op van de overall-kwaliteit en voorzien de uitkomsten in ontwikkel-/verbeterpunten die idealiter hun weg terugvinden in vakbekwaamheids- en landelijke leerprogramma's.

De Staat van Netcentrisch werken bestaat uit drie vragenlijsten die ieder een ander aspect van de netcentrische werkwijze belichten:

1. Hoe is de netcentrische werkwijze *geborgd* binnen de reguliere bedrijfsvoering van de organisatie?
2. Hoe worden *risico's en kwetsbaarheden* op netcentrische wijze beheerst?
3. Hoe worden *crises* op netcentrische wijze beheerst?

Meer informatie over deze vragenlijsten of een link om deze online in te vullen? Neem contact op met de adviseurs netcentrisch werken of via netcentrischwerken@nipv.nl.

Vakbekwaamheid

Om de kwaliteit van alle informatiefunctionarissen te waarborgen en vakbekwaam te blijven, is het raadzaam om netcentrisch werken in het OTO-programma op te nemen. Vanuit het NIPV is een oefeninspiratiebank ontwikkeld waarin veel leuke en inspirerende oefeningen zijn opgenomen. Het is een besloten groep waarvoor toegang aangevraagd kan worden via netcentrischwerken@nipv.nl.

Daarnaast kan tijdens deze oefeningen vragenlijst 3 van de Staat van Netcentrisch werken worden ingevuld. Deze kunnen door collega's uit dezelfde organisatie of collega's uit een buurorganisatie worden ingevuld. Indien wenselijk kunnen collega's vanuit het NIPV langskomen om eens mee te kijken en feedback te geven.

Fallback beoefenen

Het kan voorkomen dat het ondersteunende systeem LCMS tijdelijk niet toegankelijk is, of dat de internetverbinding niet werkend is. In die gevallen moet een organisatie terugvallen op andere communicatiemiddelen om netcentrisch informatie met partners uit te wisselen. Het is goed om hier tijdens de implementatie al over na te denken en vooral daarna regelmatig te oefenen. In het [Handboek Informatiemanagement Crisisbeheersing](#) is een hoofdstuk opgenomen met meer uitleg over dit onderwerp en tips voor organisaties hoe dit op te vangen.

Bijlagen

Bijlage 1: Voorbeeld Processchema in fases

	Opzet gezamenlijk project	☒ Status
	> Doel, investeringen, resultaat en verwachtingen helder	☐
	> Plenaire start	☐
	> Acties vaststellen: welke inbreng nodig, wanneer en van wie?	☐
	Opstellen blauwdruk	☒ Status
	A. Organisatie (hoe ziet je Informatieorganisatie eruit, structuur, functionarissen)	☐
	B. Processen (melding en alarmering, op en afschaling, L&C, IM)	☐
	C. Techniek (LCMS, ICT-voorzieningen, fallback procedure)	☐
	D. Mens (taal, cultuur, kunnen en willen delen, vakbekwaam worden en blijven)	☐
	Inrichten organisatie en LCMS	☒ Status
	A. Inrichten van de organisatie	☐
	B. Aanstellen van mensen	☐
	C. Toepassen en bijstellen van de werkwijze	☐
	Opleiden	☒ Status
	A. Informatiemanagers en ICO's	☐
	B. Leidinggevenden/ voorzitters	☐
	C. De leden van het team	☐
	Operationeel gaan (en blijven)	☒ Status
	A. Trainen	☐
	B. Oefenen	☐
	C. Go-live oefening	☐
	D. D. Stay-live	☐

Bijlage 2:

Stappenplan aanschaf en inrichting Techniek

Actie	Actiehouder
Offerte aansluiten netcentrisch werken met LCMS	Crisispartner, NIPV (productmanager LCMS)
Afsluiten Dienstverleningsovereenkomst (DVO)	Crisispartner, NIPV (productmanager LCMS)
Zoek binnen je organisatie de IdP-beheerder (meestal ICT/servicedesk) op voor toegang tot het LCMS via de TGV	Crisispartner, NIPV (Productmanager TGV, LFB en adviseur Netcentrisch werken)
Mogelijkheden bespreken voor alternatieve/ besloten koppeling met het LCMS	Crisispartner, NIPV (Productmanager Diginetwerk en adviseur Netcentrisch werken)
Bepalen organisatiebeheerders	Crisispartner
Registratieformulier Organisatiebeheerders LCMS invullen en ondertekenen	Crisispartner, NIPV (Landelijk Functioneel beheer - LFB)
Opstellen formats en templates	Crisispartner, Implementatieadviseur, NIPV adviseert over NCW-werkwijze
Volgen organisatiebeheerderstraining (sjablonen worden tevens aangemaakt)	Crisispartner, NIPV (LFB)
Gebruikerslijst opstellen	Crisispartner
Gebruikers toevoegen door organisatiebeheerders	Crisispartner
Autorisatieplan (profielen) inrichten en uitvoeren	Crisispartner, NIPV (LFB)
Opstellen verwerkingsovereenkomst LCMS	Crisispartner, NIPV (productmanager LCMS)
Afspraken maken over functioneel beheer (functioneel beheerplan)	Crisispartner, NIPV (LFB)
Opleiden, trainen, oefenen IM-functionarissen in NCW-werkwijze en LCMS	Crisispartner, Implementatieadviseur
Gebruik LCMS tijdens Go-live oefening	Crisispartner, Implementatieadviseur Adoptiepartner en NIPV (waarneming netcentrisch werken)

Bijlage 3:

Vragenlijst 3 - Staat van Netcentrisch Werken

Versie 2.1 (laatst bijgewerkt 16-1-2023)

Deze vragenlijst betreft de lijst die idealiter wordt getest tijdens een oefening. De vragen zijn ingedeeld in de volgende categorieën:

- > Netwerkvorming
- > Eigen beelden
- > Rolinvulling
- > Procesverloop
- > Informatie-ondersteunde oordeels- en besluitvorming
- > Technische middelen

Per categorie zijn de kernvragen gemarkeerd met een ● (bullet).

Waarnemingsvragen	Toelichting
Netwerkvorming	
1. ● Houdt het team een overzicht van mogelijke stakeholders bij?	Wordt door het team bepaald welke organisaties door de gebeurtenis in hun belangen en verantwoordelijkheden worden geraakt?
2. Wordt per organisatie uit de netwerkanalyse geregeld overwogen of en op welke wijze deze bij het team wordt betrokken?	Organisaties die in hun belangen en verantwoordelijkheden worden geraakt door de gebeurtenis moeten mogelijk ook bij de crisisorganisatie worden betrokken. In hoeverre wordt hier systematisch bij stilgestaan?
3. Worden de verantwoordelijkheden van de betrokken partijen gerespecteerd?	Zijn de verantwoordelijkheidsgebieden van de verschillende teams goed ten opzichte van elkaar afgebakend en wordt deze afbakening ook gerespecteerd? Komen teams – bijvoorbeeld gezien het feit dat informatie breed wordt gedeeld – niet in de verleiding zich bezig te houden met waar andere teams verantwoordelijkheid voor zijn?
Eigen beelden	
4. ● Wordt een actueel eigen beeld bijgehouden dat past bij het perspectief dat het team op de gebeurtenis heeft?	Dit eigen beeld geeft uitdrukking aan het perspectief dat het betreffende team heeft op de gebeurtenis. Dit perspectief is afgeleid van de taken en verantwoordelijkheden van het team. Zie ook Artikel 2.4.2 Besluit veiligheidsregio's . Naar de letter heeft het Besluit veiligheidsregio's slechts betrekking op veiligheidsregio's. Het artikel waarnaar wordt verwezen geeft echter goed uitdrukking aan de breder toepasbare geest van netcentrisch werken.
5. ● Wordt er een overkoepelend situatiebeeld onderhouden?	Het situatiebeeld geeft een beknopt en actueel overzicht van het perspectief dat een organisatie heeft op de gebeurtenis. Een situatiebeeld dient ook deelbaar te zijn met en begrijpelijk te zijn voor organisaties waarmee wordt samengewerkt.
6. ● Wordt geo-gerelateerde informatie in een geografisch beeld ondergebracht?	Geo-gerelateerde informatie is het beste te interpreteren door de lezer als het via het geografische beeld wordt gedeeld.

Waarnemingsvragen	Toelichting
7. ● Is het eigen beeld, zowel tekstueel als geografisch, overzichtelijk en thematisch?	Het beeld dient een duidelijk overzicht te geven van het perspectief dat het team op de gebeurtenis heeft. In het tekstuele beeld geeft een thematische indeling van het beeld goed uitdrukking aan dat perspectief. Een thema is een aspect van de gebeurtenis dat de aandacht van het team heeft.
8. ● Is het eigen beeld, zowel tekstueel als geografisch, actueel?	De actuele situatie dient te worden getoond en verouderde informatie dient regelmatig uit het beeld te worden verwijderd. In Artikel 2.2.4 en Artikel 2.4.2 Besluit veiligheidsregio's worden op dit punt de volgende eisen gesteld: ➢ Binnen vijf minuten nadat is vastgesteld dat er moet worden opgeschaald is, op grond van de beschikbare gegevens, een zo volledig mogelijke beschrijving van het incident beschikbaar. ➢ Gegevens worden vervolgens nadat zij beschikbaar zijn binnen tien minuten verwerkt in het eigen beeld en voor zover mogelijk geverifieerd. Naar de letter heeft het Besluit veiligheidsregio's slechts betrekking op veiligheidsregio's. Het artikel waarnaar wordt verwezen geeft echter goed uitdrukking aan de breder toepasbare geest van netcentrisch werken.
9. Is de informatie in het beeld traceerbaar naar de informatiebron?	Is – impliciet of expliciet – duidelijk wat de bron van de informatie is?
10. Bevat het eigen beeld informatie over de situatie?	Hierbij gaat het zowel over de gebeurtenis zelf, over de gevolgen ervan en over de gevolgen van de gevolgen, etc. Indien relevant kan ook de oorzaak worden beschreven.
11. Bevat het eigen beeld informatie over genomen maatregelen?	Het betreft hier maatregelen die genomen zijn of worden om de situatie te beheersen of in het kader van de bestrijding van de gevolgen van de gebeurtenis.
12. Bevat het eigen beeld informatie over beoogde effecten?	Het betreft hier effecten die worden beoogd om de situatie te beheersen of om de gevolgen van de gebeurtenis te bestrijden.
13. Is de informatie in het beeld gevalideerd, tenzij expliciet anders aangegeven?	Wordt de gebeurtenis feitelijk in het beeld beschreven, ontdaan van aannames, meningen, vermoedens en geruchten? Waar aannames, meningen, vermoedens en geruchten relevant zijn, dienen ze expliciet als zodanig te worden gekwalificeerd.
14. Geeft het beeld op hoofdlijnen het historische verloop van de ontwikkelingen weer?	Het beeld moet niet het karakter van een journaal krijgen, maar het globale historische verloop kan wel relevant zijn in het kader van de beeldvorming.
15. Geeft het beeld op hoofdlijnen het te verwachten (toekomstig) verloop van de ontwikkelingen weer?	Een prognose van het te verwachten toekomstig verloop van de ontwikkelingen op de korte termijn (denk aan weersontwikkelingen) is een belangrijk onderdeel van de beeldvorming.

Waarnemingsvragen	Toelichting
Rolinvulling	
16. ● Is de informatiefunctionaris een volwaardige gesprekspartner van zijn teamleider?	De informatiefunctionaris is degene aan wie de uitvoering van de beeldvorming is toegewezen. Krijgt hij het daarbij passende podium en gebruikt hij dat ook?
17. Wordt de teamleider gepositioneerd als degene die eindverantwoordelijk is voor het geheel?	Maakt de teamleider duidelijk dat hij integraal verantwoordelijk is voor leiding & coördinatie én de inhoud van het beeld?
18. Ondersteunt de teamleider de informatiefunctionaris in zijn verantwoordelijkheid voor het informatiemanagement?	De teamleider neemt zijn verantwoordelijkheid om de informatiefunctionaris in het team te positioneren als verantwoordelijk voor informatiemanagement.
19. Concentreren de informatiefunctionarissen zich op het delen en laten stromen van informatie, waarbij ze de informatie-inhoud aan inhoudsdeskundigen overlaten?	Het lostrekken van data en informatie van de kennis en kunde die nodig zijn om ze te interpreteren, kan misleidende beelden opleveren. Informatiefunctionarissen hebben die kennis en kunde niet allemaal zelf in huis.
20. Is het helder welke persoon welke informatievragen oppakt?	Als een vraag wordt geformuleerd in het kader van de beeldvorming, wordt bij die vragen dan ook afgesproken wie verantwoordelijk is voor het beantwoord krijgen van de vraag?
Procesverloop	
21. ● Wordt het beeldvormingsproces gevoed vanuit de informatiebron(nen)?	Om een beeld zo betrouwbaar mogelijk te houden moet informatie vroegtijdig en dicht bij de bron worden ingevoerd en bijgehouden.
22. ● Worden de actuele beelden breed binnen de crisisorganisatie gedeeld?	Informatie dient breed te worden gedeeld en relevantie van informatie dient in beginsel aan de ontvanger te worden overgelaten.
23. ● Is voortdurend duidelijk wie de regie voert over de beeldvorming?	Eén informatiefunctionaris voert regie over de beeldvorming. Welke dat is kan in de loop van de tijd wel verschuiven. Te allen tijde moet duidelijk zijn wie de regievoerend functionaris is.
24. ● Stemmen de teamleider en de informatiefunctionaris (ruim) voorafgaand aan het overleg af over de 'command intent', de overlegdoelen en de beeldvormingsthema's?	Om een overleg informatie-gestuurd te doen zijn, verdient het de aanbeveling dat de informatiefunctionaris en de teamleider voorafgaande aan ieder overleg gezamenlijk de 'command intent', de doelen van het overleg en de beeldvormingsthema's vaststellen. Het is belangrijk om deze zaken regelmatig te actualiseren omdat ze zich met het verloop van het proces ook ontwikkelen.
25. Spreekt de informatiefunctionaris andere functionarissen aan op hun verantwoordelijkheid informatie te delen?	Hierbij gaat het vooral over functionarissen binnen zijn eigen team.
26. Spreekt de regievoerend informatiefunctionaris de andere informatiefunctionarissen aan op hun verantwoordelijkheid informatie te delen en hun eigen beeld actueel te houden?	Vult de regievoerend informatiefunctionaris de regierol ook adequaat in?

Waarnemingsvragen	Toelichting
27. Wordt actief informatie gehaald?	Worden lacunes in het beeld expliciet benoemd en wordt er actie ondernomen om deze lacunes in te vullen?
28. Heeft de informatiefunctionaris regelmatig contact met andere informatiefunctionarissen om de situatie beter te begrijpen?	Onder regie van de regievoerend informatiefunctionarissen is het collectief van informatiefunctionarissen belast met het onderhouden van een samenhangend beeld. Daarbij past dat ze onderling geregeld contact hebben om ervoor te zorgen dat de organisatie als geheel een gedeeld totaalbeeld heeft. Zie ook Artikel 2.4.1 Besluit veiligheidsregio's . Naar de letter heeft het Besluit veiligheidsregio's slechts betrekking op veiligheidsregio's. Het artikel waarnaar wordt verwezen geeft echter goed uitdrukking aan de breder toepasbare geest van netcentrisch werken.
Informatie-ondersteunde oordeels- en besluitvorming	
29. ● Stelt de teamleider bij de gemeenschappelijke oordeels- en besluitvorming het gedeelde beeld centraal en vormen de thema's de rode draad?	Geeft de teamleider het gedeelde beeld een centrale rol in overleggen? Wordt ieder overleg bijvoorbeeld gestart met het presenteren van het actuele beeld? Gebruikt hij de thema's en een tijdlijn om de oordeelsvorming te ondersteunen?
30. ● Worden beeldvorming, oordeelsvorming en besluitvorming van elkaar gescheiden door de teamleider?	Is de vergaderstructuur helder in die zin dat beeld-, oordeels- en besluitvorming goed ten opzichte van elkaar worden afgebakend door de teamleider?
31. Richt het team zich op de aspecten die passen bij het coördinatie-niveau van het team?	Een strategisch team richt zich op beleid en belangen, een tactisch team richt zich op effecten en capaciteiten en een operationeel team richt zich op middelen en acties.
32. Worden door het scenarioteam integrale scenario's ontwikkeld op basis van doelstelling en randvoorwaarden van de operationeel leider?	Deze vraag is alleen van toepassing bij teams op het tactische niveau.
33. Worden acties en besluiten in het beeld verwerkt?	Hierbij gaat het om besluiten en bijbehorende acties die aan functionarissen worden toebedeeld.
Technische middelen	
34. ● Wordt er gebruik gemaakt van de Landelijke Voorziening Crisisbeheersing voor het breed delen van actuele beelden?	Het snel en breed delen van informatie kan feitelijk alleen als er gebruik wordt gemaakt van technische voorzieningen. Zie ook Artikel 22 Wet veiligheidsregio's . De Landelijke Voorziening Crisisbeheersing is de concretisering van dit wetsartikel. Naar de letter heeft de Wet veiligheidsregio's slechts betrekking op veiligheidsregio's. De stelselverantwoordelijkheid op het gebied van crisisbeheersing straalt echter uit naar de veiligheidspartners.
35. Functioneren de technische middelen ter ondersteuning van informatiemanagement naar behoren?	Worden de beschikbaarheid, vertrouwelijkheid en integriteit van de informatie gewaarborgd?