

Bedrijfscontinuïteitsplan Cyber

Regionale Dienst Werk en Inkomen Kromme Rijn Heuvelrug

Dit Bedrijfscontinuïteitsplan Cyber bevat een beschrijving van de kritische bedrijfsprocessen van de RDWI; een analyse van de risico's die voor dezen een bedreiging vormen; strategieën die bijdragen aan de continuïteit op technologisch, operationeel en communicatief vlak; een uiteenzetting van de taak- en rolverdeling binnen de eigen cybercrisisorganisatie; en een beschrijving van het déchargeproces om als organisatie, na een (cyber-)crisis te hebben doorstaan, terug te keren naar de normale gang van zaken.

Inhoudsopgave

1. Inleiding.....	5
1.1 Doel.....	5
1.2 Crisisdefinitie.....	5
1.3 Definitie bedrijfscontinuïteitsmanagement.....	6
1.4 Samenhang met andere plannen en protocollen.....	6
1.5 Verantwoordelijkheid en versiebeheer.....	6
2. Kritische bedrijfsprocessen	7
2.1 Definitie en criteria	7
2.2 Link met IT	7
2.3 Kritische bedrijfsprocessen aan de hand van kernthema's.....	7
3. Dienstverlening	9
3.1 Kritische bedrijfsprocessen Dienstverlening	9
3.2 Bereikbaar zijn voor indienen aanvragen	9
3.2.1 Continuïteitsstrategie bereikbaar zijn voor indienen aanvragen	10
3.3 Bereikbaar zijn voor contact met inwoners	12
3.3.1 Continuïteitsstrategie bereikbaar zijn voor contact met inwoners	12
4. Betalingsverkeer	14
4.1 Kritische bedrijfsprocessen Betalingsverkeer	14
4.2 Uitbetalen bijstandsuitkeringen	14
4.2.1 Veegrans uitbetalen bijstandsuitkering	15
4.2.2 Continuïteitsstrategie uitbetalen bijstandsuitkering	16
4.3 Uitbetalen bijzondere bijstandsuitkeringen.....	17
4.3.1 Continuïteitsstrategie uitbetalen bijzondere bijstandsuitkeringen	18
4.4 Verstrekken broodnoodvoorschot	19
4.4.1 Continuïteitsstrategie verstrekken broodnoodvoorschot.....	19
4.5 Uitbetalen salarissen WSW'ers	20
4.5.1 Continuïteitsstrategie uitbetalen salarissen WSW'ers.....	20
4.6 Uitbetalen leefgeld en vaste lasten	21
4.6.1 Continuïteitsstrategie uitbetalen leefgeld en vaste lasten	22
4.7 Uitbetalen salarissen eigen werknemers	23
4.7.1 Continuïteitsstrategie uitbetalen salarissen eigen werknemers.....	24

5. Cybercrisisorganisatie	26
5.1 Wanneer komt de cybercrisisorganisatie in actie?	26
5.2 Cybercrisisorganisatie: Bestuurlijk en operationeel	26
5.3 Bestuurlijk crisisteam – het Bestuurlijk Kernteam (BKT)	27
5.3.1 Rol- en taakverdeling BKT	27
5.4 Operationeel crisisteam – het Lokaal Operationeel Kernteam (L-OKT)	28
5.4.1 Rol- en taakverdeling L-OKT	28
5.5 Regionale cybercrisisrespons	29
5.6 Afspraken en procedures bijeenkomen BKT en L-OKT	30
5.7 Toewijzing namen aan rollen BKT en L-OKT	31
6. Communicatie	32
6.1 Communicatie als cruciaal component cybercrisisbeheersing	32
6.1.1 Crisiscommunicatie – Wanneer start je hiermee?	32
6.1.2 Crisiscommunicatie – Tot wie richt je je?	32
6.1.3 Crisiscommunicatie – Wat communiceer je?	33
6.1.4 Crisiscommunicatie – Rollen en verantwoordelijkheden	33
6.1.5 Crisiscommunicatie – Communicatiemiddelen	34
7. Décharge – Terug naar normaal	35
7.1 Doel déchargeproces	35
7.2 Sein start déchargeproces	35
7.3 Communicatie start déchargeproces	35
7.4 Evaluatie	35
7.4.1 Inhoudelijke evaluatie	36
7.4.2 Evaluatie communicatieproces	36
7.5 Debriefing	36
B1. Overzicht crisisteamleden	37
B1.1 Lijst BKT-leden	37
B1.2 Lijst L-OKT-leden	37
B2. Contactgegevens crisisteamleden	38
B2.1 Lijst contactgegevens BKT-leden	38
B2.2 Lijst contactgegevens L-OKT-leden	38
B3. Contactgegevens leveranciers en andere partijen	39

B3.1 Lijst contactgegevens externe leveranciers	39
B3.2 Lijst contactgegevens andere partijen	39
B4. Samenvatting	40
B4.1 Schematisch overzicht kritische bedrijfsprocessen	40

1. Inleiding

1.1 Doel

Het Bedrijfscontinuïteitsplan Cyber heeft als doel om de kritische bedrijfsprocessen van de organisatie en de waarborging daarvan helder uiteen te zetten, om zodoende te garanderen dat deze zo goed mogelijk kunnen blijven functioneren, óók als er een incident of een crisis is die de organisatie treft. Verder geeft het Bedrijfscontinuïteitsplan Cyber ook een beschrijving van de interne cybercrisisorganisatie, inclusief de rol- en taakverdeling hierbinnen, om zo te waarborgen dat de organisatie adequaat handelt indien dezelfde kritische bedrijfsprocessen in het geding komen door een (cyber-)crisis.

Het Bedrijfscontinuïteitsplan Cyber is geschreven in opdracht van de Regionale Dienst Werk en Inkomen Kromme Rijn Heuvelrug en opgesteld volgens de richtlijnen die de Informatiebeveiligingsdienst (IBD) heeft meegegeven in haar uiteenzetting van *Business Continuity Management*¹. De IBD is een onderdeel van de Vereniging voor Nederlandse Gemeenten (VNG). In het Bedrijfscontinuïteitsplan Cyber wordt dan ook meerdere keren verwezen naar andere documenten van de IBD en de VNG.

1.2 Crisisdefinitie

In de handreiking *Bedrijfscontinuïteitsmanagement* van de Vereniging voor Nederlandse Gemeenten (VNG) wordt er onderscheid gemaakt tussen de termen 'ongewenste gebeurtenis', 'incident', en 'crisis'; ieder variërend in impact, complexiteit en de manier van beheersbaarheid.

Een ongewenste gebeurtenis is een zorg of een probleem met mogelijke gevolgen voor de organisatie, maar die geen onmiddellijke dreiging vormt voor de continuïteit van de bedrijfsvoering. Voorbeelden hiervan die de VNG geeft zijn onder meer een mislukte back-up, of een gebruiker die geblokkeerd is vanwege te veel foutieve aanmeldpogingen. Een incident is een gebeurtenis die de normale bedrijfsvoering verstoort en onmiddellijke aandacht vereist om verdere escalatie te voorkomen. Voorbeelden hiervan die de VNG geeft zijn onder meer een tijdelijke uitval van een ICT-systeem, of stroom.

Een crisis is een abnormale of uitzonderlijke gebeurtenis of reeks gebeurtenissen die een ernstige bedreiging vormt voor het functioneren van de organisatie en haar kritische bedrijfsprocessen. Tijdens een crisis worden (mogelijk) de continuïteit van de dienstverlening, de veiligheid van de mensen en de reputatie van de organisatie ernstig bedreigd. Besluitvorming vindt dan vaak plaats onder (een gevoel van) tijdsdruk, incomplete informatie en onzekerheid. Voorbeelden hiervan die de VNG geeft zijn een grootschalige cyberaanval, een natuurramp, of ernstige reputatieschade.

In het Bedrijfscontinuïteitsplan Cyber wordt ingezoomd op de waarborging van kritische bedrijfsprocessen als de interne bedrijfsvoering getroffen wordt door een crisis.

¹ <https://www.informatiebeveiligingsdienst.nl/business-continuity-management-bcm/>

1.3 Definitie bedrijfscontinuïteitsmanagement

‘Incidentmanagement’ behandelt de dagelijkse operationele verstoringen, terwijl ‘crisismanagement’ het geheel van de organisatorische voorzieningen wil managen om zodoende grootschalige en complexe bedreigingen aan te pakken. De plannen en protocollen die uit deze twee takken van management voortvloeien, kunnen samengevoegd en geïntegreerd worden in bedrijfscontinuïteitsmanagement.

Bedrijfscontinuïteitsmanagement is een beheerproces dat erop gericht is om de continuïteit van de meest kritische bedrijfsprocessen te garanderen, ongeacht de omstandigheden. Bij onderbreking van één of meerdere van deze kritische bedrijfsprocessen is het doel om de duur van de verstoring tot een minimum te beperken.

1.4 Samenhang met andere plannen en protocollen

Naast het Bedrijfscontinuïteitsplan Cyber heeft de RDWI ook een aantal andere plannen en protocollen opgesteld. Zo staat in het *Calamiteitenplan* de handelwijze bij brand beschreven, waarborgt het *Veiligheidsprotocol Dienstverlening en Agressie* de veiligheid van de medewerkers in relatie tot de inwoners en beschrijft het *Fysiek Veiligheidsplan* hoe de toegang tot het gebouw geregeld is. Verder zoekt dit Bedrijfscontinuïteitsplan Cyber ook overeenkomsten met het *Regionaal Crisisplan* van de Veiligheidsregio Utrecht en het *Cyber Crisisplan* van de RID. In dit Bedrijfscontinuïteitsplan Cyber wordt hier dan ook meerdere malen naar verwezen en is hier aansluiting mee gezocht.

De RDWI is een gemeenschappelijke regeling tussen de gemeenten Bunnik, De Bilt, Zeist, Utrechtse Heuvelrug, en Wijk bij Duurstede. Hierbinnen is de RDWI onder andere de uitvoeringsorganisatie voor de Wet gemeentelijke schuldhulpverlening, de Participatiewet, en aanpalende wetgeving. Verwijzingen in dit Bedrijfscontinuïteitsplan Cyber naar dergelijke wettelijke regelingen doelen dan ook op de uitvoering ervan door de RDWI namens deze vijf gemeenten.

1.5 Verantwoordelijkheid en versiebeheer

Degene die vanuit de RDWI deelneemt aan het Strategisch Opdrachtgevers Overleg (SOO) van de regionale samenwerking is degene die verantwoordelijk is voor het halfjaarlijks (laten) reviewen en (laten) updaten van het Bedrijfscontinuïteitsplan Cyber.

Datum:	Versie en Beschrijving:	Naam Uitvoerder:
09-09-25	0.95 – Oplevering BCP aan MT	M.C. van Roon

2. Kritische bedrijfsprocessen

2.1 Definitie en criteria

De VNG adviseert om bij het prioriteren van de bedrijfsprocessen een klantgerichte benadering te hanteren. Dit houdt in dat 'het belang van bedrijfsprocessen bepaald wordt aan de hand van het belang dat een gebruiker of afnemer heeft bij de continuïteit van een bepaald(e) dienst of product'.

Er is sprake van een kritisch bedrijfsproces als het voldoet aan één of meerdere van de volgende criteria:

- Het betreft de uitvoering van wetgeving.
- Het raakt de continuïteit van de dienstverlening van de organisatie.
- Het bedrijfsproces is cruciaal voor andere (kritische) bedrijfsprocessen.
- Het bedrijfsproces moet binnen 24 à 48 uur weer beschikbaar zijn.
- Uitval van het bedrijfsproces brengt ernstige schade toe aan het imago van de organisatie.
- Uitval van het bedrijfsproces heeft impact op maatschappelijke ontwrichting.
- Uitval van het bedrijfsproces leidt tot grote (herstel-)schade of inkomstenderving met grote financiële consequenties.

2.2 Link met IT

Veel IT-systemen zijn door de RDWI ondergebracht bij de RID Utrecht. Omdat de RDWI een deelnemer is aan deze gemeentelijke regeling, is de RID de verantwoordelijk voor het draaiende houden van het netwerk, de telefonie, de servers, de primaire en de ondersteunde software, de kantoorautomatisering, de koppelvlakken, de back-ups, de *restore* en de uitwijk. De RID is ook verantwoordelijk voor het periodiek testen, en waar nodig updaten van deze voorzieningen. Daarnaast zijn er ook externe leveranciers waarmee de RDWI contractuele afspraken heeft over de levering van IT-applicaties en IT-systemen. In dit Bedrijfscontinuïteitsplan Cyber worden deze leveranciers specifiek benoemd. In *Bijlage 3* staan de contactgegevens van deze leveranciers vermeld.

2.3 Kritische bedrijfsprocessen aan de hand van kernthema's

De IBD geeft zelf een opsomming van een zeventiental kritische bedrijfsprocessen voor gemeenten², waarbij de RDWI vanuit de deelnemende gemeenten (zie 1.4) een uitvoerende taak heeft voor vier van deze kritische bedrijfsprocessen. Deze zijn, samen met de overige kritische bedrijfsprocessen die de RDWI zelf nog verder kent, in dit Bedrijfscontinuïteitsplan Cyber onderverdeeld in twee kernthema's: 'Dienstverlening' en 'Betalingsverkeer'.

² <https://www.informatiebeveiligingsdienst.nl/product/top-kritische-bedrijfsprocessen/>

In dit Bedrijfscontinuïteitsplan Cyber worden acht kritische bedrijfsprocessen beschreven. Deze zijn hieronder opgesomd. Voor de eerste twee kritische bedrijfsprocessen geldt dat zij bij het kernthema Dienstverlening horen. De overige zes kritische bedrijfsprocessen zijn onder het kernthema Betalingsverkeer geschaard.

- Bereikbaar zijn voor het indienen van aanvragen
- Bereikbaar zijn voor contact met inwoners
- Uitbetalen van de bijstandsuitkeringen
- Uitbetalen van de bijzondere bijstandsuitkeringen
- Verstrekken van een broodnoodvoorschot
- Uitbetalen van de salarissen van de werknemers in de Sociale Werkvoorziening
- Uitbetalen van het leefgeld en de vaste lasten in het kader van budgetbeheer
- Uitbetalen van de salarissen van de eigen werknemers

In dit Bedrijfscontinuïteitsplan Cyber is er een hoofdstuk aan beide kernthema's gewijd. Hierin worden voor elk kritisch bedrijfsproces dat bij dat kernthema hoort een procesbeschrijving, een inschatting van het grootste risico, een maximale tolerantie van uitval, én de continuïteitsstrategie voor het waarborgen van dat kritische bedrijfsproces gegeven. Het kernthema Dienstverlening wordt behandeld in *Hoofdstuk 3*, terwijl het kernthema Betalingsverkeer in *Hoofdstuk 4* is uiteengezet. Ná de beschrijving van de cybercrisisorganisatie, te vinden in *Hoofdstuk 5*, wordt Communicatie, wat ook één van de kritische bedrijfsprocessen is volgens de IBD, uitgewerkt in *Hoofdstuk 6*. Dit is gedaan omdat communicatie een kernonderdeel is van het werk dat er in de cyberorganisatie verricht wordt.

3. Dienstverlening

3.1 Kritische bedrijfsprocessen Dienstverlening

Binnen de RDWI bedrijft men twee takken van sport. Enerzijds biedt zij hulp bij werk, re-integratie, inburgering en schuldhulpverlening, anderzijds betaalt zij voorschotten, uitkeringen en salarissen uit. Bij de dienstverlening rondom werk en re-integratie staat het benaderbaar en bereikbaar zijn voor inwoners en het begeleiden van diezelfde inwoners centraal. Deze bedrijfsprocessen zijn van kritisch belang, omdat de RDWI het zich niet kan veroorloven om deze diensten minstens één week geen doorgang te laten vinden. Het bieden van begeleiding aan inwoners, bijvoorbeeld tijdens een traject voor schuldhulpverlening, is géén kritisch bedrijfsproces. De waarborging hiervan staat overigens wel beschreven in onder meer het *Calamiteitenplan* en het *Fysieke Veiligheidsplan*.

Binnen het kernthema Dienstverlening zijn er dus twee kritische bedrijfsprocessen te benoemen. Voor ieder van deze zijn het proces, de gebruikte (IT-)systemen, de risico's, de maximale tolerantie van uitval, en de continuïteitsstrategieën ervoor beschreven:

- Bereikbaar zijn voor het indienen van aanvragen
- Bereikbaar zijn voor contact met inwoners

3.2 Bereikbaar zijn voor indienen aanvragen

De RDWI is verantwoordelijk voor het bereikbaar zijn voor inwoners van de aangesloten gemeenten die een aanvraag willen indienen voor één of meerdere van de volgende wettelijke regelingen:

- Een bijstandsuitkering
- Een broodnoodvoorschot
- Een bijzondere bijstandsuitkering
- Een levensonderhoudsuitkering in het kader van de Participatiewet

Voor inwoners zijn er drie wijzen waarop zij de RDWI kunnen contacteren voor het indienen van een aanvraag. De meest gangbare manier is via de Snelbalie – een Centric-applicatie op de website van de RDWI waarop inwoners een dergelijke aanvraag kunnen indienen. De inwoner logt dan in op de Snelbalie met zijn DigiD, waarmee hij direct zijn persoonlijke identiteit bevestigt, vult een 'vragenboom' in en dient deze bij de RDWI in. Hiervan komt een melding, min of meer geautomatiseerd, binnen bij het team Inkomen, waarna Regisseurs Intake deze beoordelen.

In ongeveer de helft van de gevallen wordt de melding als "terecht" beoordeeld en neemt de Regisseur Intake contact op met de inwoner. Hierna krijgt de inwoner, per e-mail of via de Snelbalie, een link toegestuurd voor een aanvraagindiening, wat eigenlijk een uitgebreide aanvraag is. De inwoner dient deze uitgebreide aanvraag vervolgens wéér in via de e-mail of via de Snelbalie, waarna de Regisseur Intake het restant van de administratie voltooit.

De inwoner kan de RDWI ook telefonisch contacteren voor het indienen van een aanvraag. De telefoniste stelt enkele informerende vragen, waarna zij een papieren aanvraag per post naar de inwoner verstuurt. De inwoner vult vervolgens zelf dit aanvraagformulier in en stuurt deze per post weer terug naar de RDWI. Als de inwoner behoefte heeft aan fysieke hulp bij het indienen van een aanvraag, dan kan hij zich, als derde optie, ook melden op het kantoor van de RDWI in Zeist. Hier zit namelijk de 'formulierenbrigade' – een groep medewerkers die inwoners helpt bij het invullen en indienen van een melding of een aanvraag. Deze analoge vorm van bereikbaarheid is een wettelijke vereiste. Voor de formulierenbrigade én de papieren aanvraag geldt dat het aanvraagformulier gescand moet worden. Een RDWI-medewerker digitaliseert deze dan.

Bij het bereikbaar zijn voor het indienen van aanvragen is de toegankelijkheid van de Snelbalie het grootste risico voor de RDWI. Centric beheert deze applicatie immers en de RDWI heeft dus zelf geen invloed op het wel of niet goed functioneren van de Snelbalie. Verder is de RDWI ook afhankelijk van de RID, die de telefoonlijn in beheer heeft, en van de bereikbaarheid van het kantoorpand zelf.

De RDWI hanteert een tolerantie van uitval van maximaal 72 uur voor het kunnen aanvragen van een uitkering, ongeacht de wijze waarop die aanvraag binnenkomt. De enige uitzondering hierop is de aanvraag van een broodnoodvoorschot – hier is geen tolerantie van uitval op, vanwege het acute karakter dat broodnood kenmerkt. Voor de overige aanvragen geldt het uitgangspunt dat het bestaande inwonersbestand bij de RDWI voorrang krijgt ten tijde van crisis op degenen die een nieuwe aanvraag willen indienen – wederom met uitzondering van het broodnoodvoorschot.

3.2.1 Continuïteitsstrategie bereikbaar zijn voor indienen aanvragen

De RDWI heeft vanuit de deelnemende gemeenten dus de taak overgedragen gekregen om bereikbaar en toegankelijk te zijn voor hun inwoners om ten aller tijde een aanvraag voor een bijstandsuitkering, een broodnoodvoorschot, levensonderhoud in het kader van de Participatiewet, en een bijzondere bijstandsuitkering te kunnen doen – óók ten tijde van crisis. Voor elk van deze aanvragen hanteert de RDWI een tolerantie van uitval van maximaal 72 uur, behalve bij de aanvraag van een broodnoodvoorschot – hier duldt zij geen tolerantie van uitval.

De RDWI heeft drie verschillende mogelijkheden opgezet waarmee zij bereikbaar is voor inwoners uit de deelnemende gemeenten om een aanvraag in te dienen – via de Snelbalie, telefonisch en met de formulierenbrigade. De meest gebruikte optie hiervan is de Snelbalie – een applicatie op haar eigen website waar inwoners middels het invullen van een 'vragenboom' een aanvraag voor een uitkering of een voorschot kunnen indienen, waarna deze intern door een Regisseur Intake wordt opgepakt. De Snelbalie-applicatie wordt beheerd door een externe partij, Centric, terwijl de website waar deze applicatie op draait wordt beheerd door softwareleverancier Shift2. Het voordeel hiervan is dat als er een IT-storing is bij de RDWI, dat de Snelbalie-applicatie hier dan geen hinder van ondervindt. Er kleeft hier echter ook een nadeel aan – als er een IT-probleem optreedt bij één van deze twee externe partijen, waardoor de website of de applicatie tijdelijk onbereikbaar is, dan kan de RDWI hier niks tegen doen.

Om dit probleem te ondervangen, én om inwoners te accommoderen die niet zo sterk technologisch onderlegd zijn of die simpelweg behoefte hebben aan menselijk contact bij het doen van een aanvraag, heeft de RSD ook twee andere opties om bereikbaar te zijn voor inwoners om aanvragen voor uitkeringen en voorschotten in te dienen. Zij is namelijk ook bereikbaar via haar telefonische nummer én fysiek op locatie.

Tijdens openingsuren is de RDWI telefonisch bereikbaar via een vast telefoonnummer wat in beheer is bij de RID. Er is altijd één telefoniste bij de receptie in het pand aanwezig, evenals een tweetal telefonisten die vanuit huis werken. De 'telefoonploeg' van de RDWI bestaat in totaal uit vijf personen, wat betekent dat zij tijdens piekmomenten – wat in de lijn der verwachtingen ligt tijdens een crisis – snel kunnen opschalen in capaciteit. Wel betekent het feit dat de RID de telefoonlijn beheert dat de RDWI buitenspel gezet wordt als er zich een probleem voordoet bij de RID. Vooralsnog heeft de RDWI ook nog geen alternatief telefoonnummer tot haar beschikking. Wel is er de mogelijkheid om een automatisch bandje te laten afspelen. Als een inwoner de RDWI in zo'n situatie belt, dan wordt hij in ieder geval geïnformeerd over het feit dat de RDWI dan tijdelijk telefonisch niet bereikbaar is.

Tot slot kan de inwoner ook terecht bij het RDWI-kantoorpand in Zeist voor een fysieke afspraak om een aanvraag voor een uitkering of een voorschot in te dienen. De inwoner wordt dan geholpen door de 'formulierenbrigade' – enkele medewerkers die de inwoner begeleiden in het correct invullen van het aanvraagformulier. Deze optie is extra prettig voor inwoners die behoefte hebben aan fysieke hulp en menselijk contact. Ook verlicht dit de druk op de telefonisten van de RDWI. Wel is dit sterk afhankelijk van de toegankelijkheid van het RDWI-kantoorpand. Bij, bijvoorbeeld, een brand kan men niet bij de formulierenbrigade langs. Wel heeft de RDWI afspraken met de gemeente Zeist en de gemeente Utrechtse Heuvelrug dat hun gemeentekantoren als uitwijklocatie dienen voor de RDWI. De formulierenbrigade zou dan ook hier naartoe kunnen uitwijken.

Alles bij elkaar opgeteld heeft de RDWI de continuïteit van dit kritische bedrijfsproces erg goed gewaarborgd. Zij biedt inwoners drie verschillende routes om een aanvraag in te dienen. Deze routes opereren bovendien los van elkaar. Dit biedt de RDWI de mogelijkheid om tijdens een crisis één van deze opties voorrang te geven. Zo kan er bijvoorbeeld bij een brand in het kantoorpand voor gekozen worden om uitsluitend aanvragen te accepteren via de Snelbalie, terwijl er bij een storing aldaar juist de voorkeur aan telefonisch contact gegeven kan worden. Wel moet deze keuze dan duidelijk aan haar eigen medewerkers én aan de inwoners gecommuniceerd worden.

3.3 Bereikbaar zijn voor contact met inwoners

De RDWI is op vier verschillende wijzen bereikbaar voor inwoners:

- Op locatie, in Zeist
- Telefonisch
- Per e-mail
- Per post

Het ontvangen van inwoners op kantoor in Zeist én het ontvangen van de papieren post zijn beiden afhankelijk van of het kantoorpand daadwerkelijk wel fysiek bereikbaar is. Alle voorschriften rondom de toegankelijkheid van het gebouw en de bijbehorende veiligheidsmaatregelen staan beschreven in het *Fysiek Veiligheidsplan*.

Voor de telefonische bereikbaarheid van de RDWI geldt dat zij tijdens openingsuren altijd bereikbaar is. Er zit één telefonist bij de receptie, terwijl de andere telefonist(en) thuis werken. Deze telefoonlijn wordt beheerd door de RID. Dit betekent dat als er iets mis is bij de RDWI, maar de RID-centrale wél nog in de lucht is, dat de RDWI-telefonisten 'gewoon' vanuit huis hun werk kunnen doen. Daarnaast is de RDWI dus ook via de e-mail bereikbaar. Medewerkers van de RDWI kunnen hun mailbox ook vanuit huis openen, mits zij toegang hebben tot de Citrix-werkomgeving. Het contact met de inwoner kan ook andersom geschieden – een RDWI-medewerker neemt dan zelf contact op met een inwoner, bijvoorbeeld vanwege mutaties in betalingen of voor het afstemmen van een volgende re-integratieafspraken.

Het grootste risico tijdens een crisis die de interne organisatie treft, is dat de communicatielijn naar de inwoners volledig wegvalt. Het kunnen contacteren en informeren van inwoners is cruciaal om desinformatie, paniek, chaos, en uiteindelijk reputatieschade, te voorkomen. Voor dit kritische bedrijfsproces geldt dan ook dat de RDWI geen tolerantie van uitval duldt.

3.3.1 Continuïteitsstrategie bereikbaar zijn voor contact met inwoners

De continuïteitsstrategie voor het bereikbaar zijn voor contact met inwoners hangt sterk samen met de hierboven beschreven continuïteitsstrategieën voor het bereikbaar zijn voor het doen van aanvragen (zie 3.2.1). Maar, waar daarbij de focus ligt op het doen van aanvragen en daar wel enige tolerantie van uitval bij wordt geduld, is dat bij het bereikbaar zijn voor contact met inwoners niet het geval – hier is nul tolerantie van uitval.

Bereikbaar zijn voor inwoners is immers cruciaal ten tijde van crisis – het informeren van bezorgde inwoners is cruciaal om desinformatie, paniek, chaos, en uiteindelijk reputatieschade te voorkomen. Dit gaat beide kanten op: de RDWI kan haar inwoners zelf inlichten over de crisis waarmee zij kampt, maar het kan ook zijn dat bezorgde inwoners zelf de RDWI contacteren omdat zij vernomen hebben dat er een crisis is.

De RDWI is normaliter voor haar inwoners op vier verschillende manieren bereikbaar: fysiek op kantoor in Zeist, telefonisch, per e-mail en per post. Laatstgenoemde optie is op het eerste oog de minst gebruikelijke tijdens een crisis – inwoners zullen behoefte hebben aan een snel antwoord op hun vragen en dan volstaat de papieren post niet.

Wel kan de RDWI ervoor kiezen om tóch papieren post bij haar inwoners te laten bezorgen, om hen zodoende op een iets persoonlijkere manier toch uitgebreid in te lichten. De ervaring leert dat sommige gemeenten hier bijvoorbeeld wel een sterke voorkeur voor hebben – juist vanwege dat persoonlijke kenmerk. Deze afweging is aan de Unitmanager Financiën, Informatiemanagement & Facilitair (FIF), die de verantwoordelijkheid over de Postkamer van de RDWI draagt.

Voor de fysieke bereikbaarheid van het kantoorpand geldt hetzelfde uitgangspunt als eerder beschreven bij de formulierenbrigade (zie 3.2.1): het wel of niet toegankelijk zijn van het kantoorpand ligt in principe buiten de invloedssfeer van de RDWI zelf – bij een brand, een gaslek of een bommelding moet het pand immers ontruimd worden. Wel heeft de RDWI afspraken gemaakt met de gemeente Zeist en de gemeente Wijk bij Duurstede dat hun gemeentekantoren als uitwijklocatie dienen voor de RDWI. Op het eerste oog lijkt die in Zeist hierin de logische optie – de RDWI is zelf namelijk al gevestigd in Zeist én de gemeente Zeist maakt geen gebruik van de RID-faciliteiten.

Contact onderhouden met inwoners per e-mail is ook een goed werkbare optie tijdens een crisis – een RDWI-medewerker kan immers vanuit huis toegang krijgen tot zijn eigen RDWI-mailbox. Zo kunnen consultants en regisseurs dus zelf blijven e-mailen met inwoners. Verder is er ook een algemene mailbox, die beheerd wordt door twee administratief medewerkers en waar ook de Postkamer toegang tot heeft. Tijdens een crisis is het aannemelijk dat het e-mailverkeer drukker is dan normaal – de Unitmanager FIF kan er dan toe besluiten dat werknemers vaker, of zelfs buiten werktijd, hun mailbox moeten bijhouden, om zo de drukte beter te managen.

Toch is de kans het grootst dat bezorgde inwoners de RDWI telefonisch zullen proberen te bereiken – bijvoorbeeld wanneer zij hun uitkering niet tijdig hebben ontvangen, of wanneer zij vernemen dat het pand is ontruimd. De RDWI is tijdens haar openingsuren altijd telefonisch bereikbaar. Normaliter zit er één telefonist aan de receptie, terwijl de andere telefonist(en) thuis werken. De 'telefonistenploeg' bij de RDWI bestaat uit vijf werknemers, wat betekent dat als de telefoon roodgloeiend staat, er vijf werknemers tegelijkertijd deze telefoontjes kunnen beantwoorden. Ieder van hen kan dit werk bovendien ook vanuit huis doen. De Unitmanager Intake, Werk & Participatie bepaalt hoeveel werknemers er gedurende een crisis dienst hebben. Ondanks dat de bezetting van de 'telefonistenploeg' dus uitstekend gewaarborgd is, kleeft er ook één risico aan de telefonische bereikbaarheid van de RDWI – de RID beheert namelijk de telefoonlijn. Dit betekent dat als er iets misgaat bij de RID-centrale, dat de RDWI dan machteloos staat – zij is dan niet meer telefonisch bereikbaar voor inwoners. Wel kan zij een automatisch bandje laten afspelen, die mededeelt dat de telefoonlijn eruit ligt.

De RDWI heeft de continuïteit van het kritische bedrijfsproces omtrent het bereikbaar zijn voor contact met inwoners erg goed geborgd. Zij zijn op vier verschillende manieren bereikbaar, waarvan er drie (per e-mail, telefonisch en fysiek op locatie) ook zeker werkbaar zijn tijdens een crisis. De RDWI kan er dan ook voor kiezen om één van deze opties voorrang te geven tijdens een crisis. Contact via de e-mail en per telefoon zijn hierbij de logische keuzes, omdat die door werknemers op afstand gedaan kunnen worden. Wel moet deze keuze dan duidelijk aan inwoners gecommuniceerd worden.

4. Betalingsverkeer

4.1 Kritische bedrijfsprocessen Betalingsverkeer

Volgens de afspraken met de vijf deelnemende gemeenten is de RDWI verantwoordelijk voor het verstrekken van voorschotten en het uitbetalen van uitkeringen. Binnen het kernthema Betalingsverkeer zijn er zes kritische bedrijfsprocessen te benoemen. Voor ieder van deze zijn het proces, de gebruikte (IT-)systemen, de risico's en de maximale tolerantie van uitval beschreven:

- Uitbetalen van de bijstandsuitkeringen
- Uitbetalen van de bijzondere bijstandsuitkeringen
- Verstrekken van een broodnodvoorschot
- Uitbetalen van de salarissen van werknemers in de Sociale Werkvoorziening
- Uitbetalen van het leefgeld en de vaste lasten in het kader van budgetbeheer
- Uitbetalen van de salarissen van de eigen werknemers

4.2 Uitbetalen bijstandsuitkeringen

In het kader van de Participatiewet voert de RDWI twee taken uit. Enerzijds begeleidt zij de groep inwoners die onder deze wetgeving valt in het actief zoeken naar mogelijkheden op de arbeidsmarkt. Dit is echter geen kritisch bedrijfsproces, omdat de RDWI het zich kan veroorloven om deze begeleiding, ten tijde van een crisis, uit te stellen.

Anderzijds keert de RDWI deze groep inwoners ook maandelijks een bijstandsuitkering uit. Deze bijstandsgerechtigden ontvangen 's ochtends op de 8^e van elke maand op hun bankrekening deze uitkering. Om te kunnen garanderen dat dit elke maand zo geschiedt, en om deze groep inwoners dus zo vastigheid te kunnen bieden in het voorzien van hun levensonderhoud, moet de RDWI op de 7^e van elke maand deze uitbetaling in gang zetten. Let wel: als de 8^e van de maand op een weekenddag valt, dan wordt het proces van het uitbetalen naar voren gehaald – de uitkeringsgerechtigden ontvangen hun bijstandsuitkering dan op de vrijdag voorafgaand aan datzelfde weekend.

Momenteel staan er iets minder dan drieduizend bijstandsuitkeringsgerechtigden in het inwonersbestand van de RDWI. Zij zijn allen verplichten om maandelijks hun inkomsten op te geven via de MijnRSD-app of via een hard-copy formulier. Voor een deel van deze groep inwoners geldt dat zij wisselende inkomsten hebben. Per uitkeringsgerechtigde wordt er bij de RDWI een "binnen"-verklaring afgegeven als zijn opgaveformulier is verwerkt. Deze ontvangen opgaveformulieren worden door de RDWI verzameld tijdens de maandrun, die plaatsvindt van de 15^e van elke maand tot de 7^e van de volgende maand. Tijdens deze maandrun is het team Uitkeringsadministratie verantwoordelijk voor het verrichten van de controles en de checks op deze formulieren.

Op de 7^e van elke maand loopt die maandrun ten einde en start men de uitkeringsrun. In de op de RID-servers draaiende Suite-applicatie worden door datzelfde team Uitkeringsadministratie de gecheckte aanvraagformulieren uitgedraaid in de vorm van een SEPA-bestand. Voor elk van de vijf deelnemende gemeenten wordt één SEPA-bestand uitgedraaid. Deze vijf SEPA-bestanden, met daarin dus het totaalbedrag per gemeente dat aan de bijstandsuitkeringen van de inwoners aldaar wordt uitbetaald, worden door het team Uitkeringsadministratie naar het team Financiën doorgestuurd.

Dit gebeurt altijd zo kort mogelijk op de uitbetalingsdeadline – namelijk tegen 18:00 uur op de 7^e van elke maand. Zo is men er zeker van dat deze *batch* aan bestanden de meest actuele informatie bevat. Het team Financiën checkt deze SEPA-bestanden diezelfde avond nog en geeft, bij goedkeuring hiervan, groen licht aan de BNG (de Bank Nederlandse Gemeenten). De BNG verwerkt de betalingen de volgende ochtend direct, waardoor de desbetreffende inwoners om 09:00 uur op de 8^e van elke maand hun bijstandsuitkering ontvangen.

Een belangrijk detail rondom dit kritische bedrijfsproces is dat het uitbetalingsproces op exact dezelfde wijze verloopt als dat bij de Leefgeldregeling Ontheemden, waarmee het leefgeld voor Oekraïners momenteel wordt uitgekeerd, het geval is. Wel zijn de data hierbij anders – de uitkeringsrun van de Leefgeldregeling Ontheemden wordt op de laatste dag van de maand gestart, waarna de BNG de betalingen de volgende ochtend, op de 1^e van de maand, verwerkt en de desbetreffende inwoners diezelfde ochtend het geld op hun rekening ontvangen.

Het grootste risico wat betreft het uitbetalen van de bijstandsuitkeringen, als ook het uitkeren van het leefgeld conform de Leefgeldregeling Ontheemden, schuilt in de korte tijdsperiode die de RDWI zichzelf verschaft om de uitkeringsrun uit te voeren – zij heeft hierin nauwelijks beweegruimte voor als het die specifieke avond toevallig fout gaat. Dit risico wordt verder vergroot door de sterke afhankelijkheid van de Suite-applicatie – zonder deze kan de RDWI namelijk geen SEPA-bestanden genereren en dus überhaupt geen betalingen aanmaken en goedkeuren.

Voor de RDWI is er, zodra de uitkeringsrun in gaat, geen tolerantie van uitval in dit proces. Elke vertraging die er dan op dat moment ontstaat, heeft een cruciale impact op het wel of niet halen van de betalingsdeadline op de dag erna. Als zij bijvoorbeeld pas op de 8^e van die maand de goedkeuring van de betalingen naar de BNG doorstuurt, dan ontvangen de inwoners hun bijstandsuitkering pas later op die dag of zelfs de dag erna. Omdat de bijstandsuitkering cruciaal is voor deze inwoners in hun levensonderhoud, kan de RDWI zich hierin geen uitval veroorloven.

4.2.1 Veegruns uitbetalen bijstandsuitkering

Wekelijks doet de RDWI op de dinsdag én de donderdag een extra check op de bijstandsuitkeringen én keurt zij directe uitkeringen goed. Bij deze zogeheten 'veegruns' wordt een *batch* aan bestanden meestal rond het middaguur aangeleverd door het team Uitkeringsadministratie aan het team Financiën. Het laatstgenoemde team moet deze *batch* vóór 14:30 uur gecheckt en ondertekend hebben, zodat de BNG de goedgekeurde betalingen diezelfde dag nog kan verwerken. Eenmalig een veegrun missen is overkomelijk, maar de RDWI kan het zich eigenlijk niet veroorloven om twee veegruns in één week te missen. De tolerantie van uitval hiervoor is dan ook maximaal 48 uur.

4.2.2 Continuïteitsstrategie uitbetalen bijstandsuitkering

Vanuit de deelnemende gemeenten heeft de RDWI de taak overgedragen gekregen om de bijstandsuitkeringen van de bijstandsgerechtigde inwoners tijdig en correct uit te betalen – óók ten tijde van een crisis. Omdat deze groep inwoners sterk afhankelijk is van de bijstandsuitkering om te voorzien in hun eigen levensonderhoud, duldt de RDWI geen tolerantie van uitval voor dit kritische bedrijfsproces.

Tijdens de maandrun verzamelt de RDWI de uitkeringsformulieren van de inwoners die recht hebben op bijstand. Deze inwoners dienen deze zelf elke maand in – dit doen zij via MijnRSD, een SAAS-applicatie die door Centric beheerd wordt, of via een hard copy-formulier. De bijstandsgerechtigden ontvangen ook elke maand een e-mail van de RDWI, waarin zij eraan herinnerd worden dat zij hun uitkeringsformulier moeten indienen. Mocht de MijnRSD-app uit de lucht zijn, dan heeft de RDWI dus nog de hard copy-formulieren als alternatief. De bijstandsgerechtigde inwoners ontvangen deze dan per post, waarna zij die ingevuld weer terugsturen naar de RDWI. Hier geldt dan wel voor dat het kantoorpand van de RDWI, of een uitwijklocatie, bereikbaar moet zijn om de post te kunnen ontvangen én verwerken. De RDWI hanteert een ruime 'indienperiode', namelijk de hele maandrun, waardoor zij zichzelf voldoende ademruimte geeft om alle uitkeringsformulieren te verzamelen. Bovendien organiseert zij ook twee keer per week veegrans (zie 4.2.1), waardoor de *batch* die ingediend wordt voor de uitkeringsrun zo actueel mogelijk is.

Het uitbetalen van de bijstandsuitkeringen is een precair bedrijfsproces, omdat het gebonden is aan strakke deadlines. Het team Uitkeringsadministratie draait op de 7^e van elke maand SEPA-bestanden, één per gemeente, met de gecheckte uitkeringsformulieren uit. Diezelfde avond checkt het team Financiën deze en keurt ze goed. De BNG betaalt de volgende ochtend de juiste bijstandsbedragen uit. Het hanteren van deze strakke tijdsplanning heeft een gegronde reden – zo biedt de RDWI zekerheid aan deze groep inwoners over wanneer zij hun geld ontvangen. Tegelijkertijd brengt dit ook grote risico's en vooral weinig beweegruimte met zich mee.

Op de 7^e van elke maand, waar de maandrun eindigt en de uitkeringsrun van start gaat, moet alles perfect verlopen. Op de Suite-applicatie, wat geleverd wordt door Centric en wat draait op de RID-servers, draait het team Uitkeringsadministratie de gecheckte en goedgekeurde uitkeringsformulieren uit in de vorm van SEPA-bestanden. De RDWI is heel sterk afhankelijk van het goed functioneren van deze Suite-applicatie. Als deze met een (tijdelijke) IT-storing kampt, kan de RDWI niet zelf SEPA-bestanden aanmaken. Dit betekent concreet ook dat de RDWI in zo'n geval geen betalingen goed kan keuren en de bijstandsgerechtigden dus hun uitkering niet ontvangen.

Alle SEPA-bestanden van de betalingen van de vorige maanden worden op een netwerkschijf opgeslagen. De RDWI kan er dus theoretisch gezien toe beslissen om eenmalig de SEPA-bestanden van de vorige maand te gebruiken als referentiekader voor de uitbetalingen van de huidige maand. Deze *work-around* is echter onwenselijk, omdat er één SEPA-bestand per gemeente wordt aangemaakt én daarin geen onderscheid gemaakt wordt tussen de verschillende regelingen en uitkeringen. Dit betekent, in combinatie met alle mutaties die er ook nog eens plaatsvinden tijdens de maandrun, dat de foutmarge hierop veel te hoog wordt.

Bij een normale gang van zaken worden de SEPA-bestanden vóór 18:00 uur via Microsoft Teams afgeleverd aan het team Financiën. Dit team checkt, in de Citrix-werkomgeving, deze SEPA-bestanden nogmaals, voordat zij groen licht geeft voor het uitbetalen van de uitkeringen door de BNG. Hiermee voldoet de RDWI direct ook aan het vier-ogenprincipe. Als de Citrix-werkomgeving niet goed functioneert, dan kan deze laatste check ook handmatig gedaan worden. Hier is het team Uitkeringsadministratie dan verantwoordelijk voor. Na het voltooien van deze laatste check zet de Unitmanager Financiën, Informatiemanagement & Facilitair (FIF) zijn handtekening onder de SEPA-bestanden. Hij verstuurt vervolgens een e-mail naar de BNG, met daarbij een HTML-bestand bijgevoegd. Dit HTML-bestand dient dan als 'bewijs' dat de SEPA-bestanden zijn uitgedraaid, gecontroleerd en goedgekeurd. Het versturen van deze e-mail hoeft niet in de Citrix-werkomgeving te gebeuren. De BNG verricht hierna de uitbetaling.

Het uitbetalen van de bijstandsuitkeringen is dus een precair kritisch bedrijfsproces waarbij de RDWI gebonden is aan strakke tijdsafspraken. De RDWI heeft dit kritische bedrijfsproces goed gewaarborgd op het vlak van *checks and balances*, met onder meer de veegrans en het vier-ogenprincipe. Bij de uitkeringsrun is de RDWI echter wel erg kwetsbaar – zij heeft namelijk geen back-upoptie voorhanden als de SEPA-bestanden niet uitgedraaid kunnen worden in de Suite-applicatie. Bovendien wordt het gebruiken van de SEPA-bestanden van de vorige maand als referentiekader door de RDWI ook als onwenselijk beschouwd. De RDWI zou er goed aan doen om een back-up te creëren, zo dicht mogelijk op de uitkeringsrun, van de uitkeringsformulieren van de huidige maand. Als de Suite-applicatie dan niet naar behoren functioneert, dan kan de RDWI teruggrijpen op een recente back-up – en op basis hiervan handmatig de uitbetalingen doen.

4.3 Uitbetalen bijzondere bijstandsuitkeringen

Inwoners met een laag inkomen die noodzakelijke kosten hebben gemaakt die zij zelf niet kunnen betalen, én die niet door andere regelingen worden gedekt, ontvangen van de RDWI een bijzondere bijstandsuitkering. Deze uitbetaling kan incidenteel zijn, bijvoorbeeld bij advocaatkosten of medische kosten, maar ook structureel, bijvoorbeeld bij de kosten voor bewindvoering bij langdurige problematiek. In dergelijke gevallen wordt de RDWI door de inwoner zelf, of door zijn begeleider, gecontacteerd met het verzoek of hij recht heeft op een bijzondere bijstandsuitkering.

Het uitbetalen van de bijzondere bijstandsuitkeringen geschiedt op dezelfde wijze als bij de bijstandsuitkeringen (zie 4.2). Het team Uitkeringsadministratie verzamelt tijdens de maandrun alle opgaveformulieren van structurele kosten en draait deze, in de Suite-applicatie, uit in dezelfde SEPA-bestanden die bij de bijstandsuitkeringen gegenereerd worden. Bij de start van de uitkeringsrun, dus op de 7^e van elke maand, worden deze SEPA-bestanden naar het team Financiën doorgestuurd. Dit team geeft hier vervolgens haar fiat op, ondertekent deze, en zet deze in het BNG-systeem. De inwoner ontvangt zijn bijzondere bijstandsuitkering dan op de 8^e van elke maand. Voor de incidentele kosten die inwoners in het kader van de bijzondere bijstand opgegeven hebben, geldt dat deze tijdens de veegrans gecontroleerd en uitgekeerd worden. Deze veegrans vinden tweemaal per week plaats – op dinsdag en op donderdag. De inwoner ontvangt de uitbetaling van deze incidentele kosten een dag later.

De sterke afhankelijkheid van de Suite-applicatie voor het uitbetalen van de bijzondere bijstandsuitkeringen vormt het grootste risico bij dit kritische bedrijfsproces – zonder de Suite-applicatie kan de RDWI namelijk zelf geen SEPA-bestanden aanmaken. Voor het uitbetalen van de structurele kosten in het kader van de bijzondere bijstand geldt dat de RDWI geen tolerantie van uitval duldt – juist ook omdat deze uitbetaling tegelijkertijd met die van de bijstandsuitkering plaatsvindt. Voor de uitbetaling van de incidentele kosten in het kader van de bijzondere bijstand geldt dat de RDWI een tolerantie van uitval van maximaal 48 uur hanteert. Hierbij heeft de RDWI namelijk nog de optie om met schuldeisers in gesprek te gaan als die hun geld niet tijdig uitgekeerd krijgen. Zeker in het geval van een crisis is de verwachting dat deze schuldeisers bereid zullen zijn om de betaling een aantal dagen uit te stellen. Dit contact met de schuldeiser verloopt vanuit de RDWI dan via een toegewezen Regisseur Inkomen.

4.3.1 Continuïteitsstrategie uitbetalen bijzondere bijstandsuitkeringen

De RDWI heeft vanuit de deelnemende gemeenten de taak overgedragen gekregen om de bijzondere bijstandsuitkeringen van de daarvoor gerechtigde inwoners tijdig en correct uit te betalen – óók ten tijde van een crisis. Een bijzondere bijstandsuitkering kan zowel een structurele betaling als een incidentele betaling zijn. Voor de structurele variant duldt de RDWI geen tolerantie van uitval, voor de incidentele variant hanteert zij een maximale tolerantie van uitval van 48 uur.

Het verzamelen en het verwerken van de bijzondere bijstandsuitkeringsaanvragen geschiedt op dezelfde wijze als bij de bijstandsuitkeringsaanvragen (zie 4.2.2). Een inwoner dient via de MijnRSD-app of via een hard copy-formulier zijn gemaakte of te maken kosten in bij de RDWI. Deze kostenopgave wordt gecontroleerd door het team Uitkeringsadministratie. Tijdens de tweewekelijkse veegrans worden de incidentele kostenopgaven in het kader van de bijzondere bijstand afgehandeld en direct uitbetaald. Voor de structurele kostenopgaven geldt dat deze, net als bij de bijstandsuitkeringen, tot en met de 7^e van elke maand worden verzameld. Deze worden op die dag vóór 18:00 uur uitgedraaid in hetzelfde SEPA-bestand als de bijstandsuitkeringen. Er wordt één overkoepelend SEPA-bestand per gemeente gegenereerd. Dit proces vindt plaats op de Suite-applicatie, wat beheerd wordt door Centric en draait op de RID-servers. Het team Financiën moet vervolgens haar fiat geven op deze SEPA-bestanden, waarna de Unitmanager FIF deze ondertekent en in het BNG-systeem zet.

Voor de waarborging van dit kritische bedrijfsproces geldt grotendeels dezelfde conclusie als bij de waarborging van het uitbetalen van de bijstandsuitkering. Het uitbetalen van de bijzondere bijstandsuitkeringen zit, mede door het runnen van de veegrans en het toepassen van het vier-ogenprincipe, qua *checks and balances* sterk in elkaar. Echter, de RDWI is voor het uitbetalen van de bijzondere bijstandsuitkeringen sterk afhankelijk van of de Suite-applicatie functioneert. Omdat de RDWI zelf geen alternatief hiervoor heeft, en dus niet zelf SEPA-bestanden kan aanmaken, is zij op dit vlak erg kwetsbaar. Ook kan zij de SEPA-bestanden van de vorige maanden niet gebruiken als referentiekader voor de uitbetaling van de huidige maand, omdat de foutmarge hierop te groot is (zie ook 4.2.2).

Net als bij het uitbetalen van de bijstandsuitkeringen (zie 4.2.2) geldt hier het devies dat het voor de continuïteit van het uitbetalen van de bijzondere bijstandsuitkeringen goed zou zijn als de RDWI een back-up van de uitbetalingsgegevens zou aanmaken die zo dicht mogelijk op de uitkeringsrun zit. Als de Suite-applicatie dan tijdens de uitkeringsrun met problemen kampt, dan kan de RDWI in ieder geval teruggrijpen op een recente back-up en op basis hiervan handmatig de uitbetalingen verrichten. Wel is er, in het geval van schuldeisers, de mogelijkheid voor een Regisseur Inkomen van de RDWI om in gesprek te gaan met diezelfde schuldeisers. De RDWI heeft als instantie namelijk een goede reputatie en menig schuldeiser zal daarom waarschijnlijk akkoord gaan met het later ontvangen van het geldbedrag dat hem verschuldigd is.

4.4 Verstrekken broodnoodvoorschot

Als een inwoner in een dermate acute financiële nood zit dat hij zijn levensnoodzakelijke voorzieningen, zoals eten of medicatie, niet kan betalen, dan kan hij een voorschot in de vorm van broodnood aanvragen. De RDWI kan dan vijftig euro cash aan die inwoner verstrekken, zodat hij zijn noodzakelijke boodschappen kan doen. Het initiatief voor een broodnoodaanvraag ligt altijd bij de inwoner, of diens begeleider.

Bij de RDWI is de afspraak dat er altijd een verantwoordelijke op kantoor aanwezig moet zijn die gevolmachtigd is om een aanvraag voor een broodnoodvoorschot goed te keuren. Dit is altijd een Unitmanager. De inwoner moet dan langskomen bij het kantoorpand om zijn broodnoodvoorschot op te halen. De fysieke bereikbaarheid van de RDWI is dan ook de belangrijkste factor, en daarmee tevens het grootste risico, voor het in stand houden van dit kritische bedrijfsproces. Bovendien is dit ook een factor waar de RDWI zelf nauwelijks tot geen invloed op heeft. Vanwege de acute aard waar broodnood door gekenmerkt wordt, duldt de RDWI hier geen tolerantie van uitval voor.

4.4.1 Continuïteitsstrategie verstrekken broodnoodvoorschot

De RDWI heeft vanuit de deelnemende gemeenten de taak overgedragen gekregen om een broodnoodvoorschot te verstrekken aan hulpbehoevende inwoners die in acute financiële nood zitten en hun levensnoodzakelijke voorzieningen, zoals eten of medicatie, niet meer kunnen betalen. De RDWI duldt hierin geen tolerantie van uitval, juist omdat een aanvraag voor broodnood zich kenmerkt door die acute hulpbehoefte.

Een broodnoodvoorschot wordt vanuit de RDWI altijd fysiek afgegeven aan de inwoner. Dit betekent dat de inwoner altijd bij het kantoorpand in Zeist moet langskomen om een aanvraag voor broodnood in te dienen én om het broodnoodvoorschot ter plekke te ontvangen. Het initiatief voor een broodnoodaanvraag ligt dus altijd bij de inwoner zelf, of diens begeleider. Een belangrijke voorwaarde die aan het verkrijgen van een broodnoodvoorschot kleef, is dat de inwoner al bekend moet zijn bij de RDWI én dat er al sprake is van een 'aanvraag in behandeling'. Alleen dan komt de inwoner in aanmerking voor een broodnoodvoorschot. Als dit niet het geval is, dan zal een medewerker van de RDWI de inwoner ter plekke helpen met het indienen van de juiste aanvraag voor een andere uitkering.

De RDWI verstrekt, als de broodnoodaanvraag gegrond is, vijftig euro cash aan de inwoner. Om dit te bekostigen heeft de RDWI een kleine voorraad cash tot haar beschikking – deze wordt bewaard in de kluis op de eerste verdieping van haar kantoorpand in Zeist. Intern is er bij de RDWI de afspraak dat er altijd een verantwoordelijke aanwezig moet zijn die gevolmachtigd is om het verlenen van dit broodnoodvoorschot goed te keuren. Een andere willekeurige medewerker mag nooit zelf de vijftig euro cash meegeven. Deze verantwoordelijke is altijd een Unitmanager.

4.5 Uitbetalen salarissen WSW'ers

In het kader van de Wet sociale werkvoorzieningen heeft de RDWI met de Biga Groep een samenwerkingsverband voor het bieden van ondersteuning aan werknemers in de Sociale Werkvoorziening (WSW) – mensen met een arbeidsbeperking die niet in bij reguliere baan terecht kunnen, maar wel in staat zijn om te werken onder aangepaste omstandigheden. Bij dit samenwerkingsverband is de Biga Groep materiaal werkgever. De RDWI is juist formeel wetgever en dus verantwoordelijk voor het uitbetalen van de salarissen van deze WSW'ers.

De Biga Groep publiceert elke 20^e van de maand één SEPA-bestand met daarin de persoons- en betaalgegevens van de werknemers in de Sociaal Werkvoorziening en zet deze in het BNG-systeem. Diezelfde dag stuurt zij, per e-mail, een beveiligde toegangssleutel naar het team Financiën van de RDWI, die de door de Biga Groep opgegeven administratie checkt. Het team Financiën zet dan diezelfde dag óf de daaropvolgende dag, dus de 20^e of de 21^e van de maand, haar handtekening onder dit SEPA-bestand in het BNG-systeem, waarna de BNG automatisch de uitbetaling van de salarissen aan de WSW'ers start.

Bij het uitbetalen van de salarissen van de WSW'ers is het grootste risico voor de RDWI haar sterke afhankelijkheid van de Biga Groep. Als de Biga Groep het SEPA-bestand niet tijdig en correct aanlevert, dan kan de RDWI haar handtekening niet hieronder zetten – en ontvangen de WSW'ers hun salarissen niet. De RDWI duldt voor dit kritische bedrijfsproces geen tolerantie van uitval, omdat zij het naar deze groep inwoners toe verplicht is om de uitbetaling op de juiste datum te doen. De WSW'ers zijn namelijk sterk afhankelijk van dit salaris om te voorzien in hun eigen levensonderhoud.

4.5.1 Continuïteitsstrategie uitbetalen salarissen WSW'ers

De RDWI is, in het kader van de Wet sociale werkvoorzieningen, verantwoordelijk voor het uitbetalen van de salarissen van de werknemers in de Sociale Werkvoorziening. Op de 20^e of 21^e van elke maand keert de RSD deze salarissen aan deze groep personen uit. De RDWI duldt hierbij geen tolerantie van uitval, omdat deze werknemers afhankelijk zijn van dit salaris om in hun eigen levensonderhoud te kunnen voorzien.

Voor de uitvoering van de Wet sociale werkvoorzieningen werkt de RDWI samen met de Biga Groep. Deze partij begeleidt de WSW'ers naar een passende baan, terwijl de RDWI als formeel wetgever 'slechts' een uitbetalingstaak heeft. De Biga Groep is ook verantwoordelijk voor de administratie en publiceert in het kader daarvan op de 20^e van elke maand één SEPA-bestand met daarin de persoons- en betaalgegevens van de

werknemers in de Sociale Werkvoorziening. Dit SEPA-bestand zet zij zelf in het BNG-systeem. Diezelfde dag ontvangt het team Financiën van de RDWI per e-mail van de Biga Groep een beveiligde toegangssleutel, waarmee zij de door de Biga Groep opgegeven administratie kan checken. Als deze e-mail niet tijdig verschijnt, dan belt de Unitmanager FIF direct de Biga Groep. Want, zonder dit SEPA-bestand kan de RDWI het uitbetalingsproces niet starten.

Hier schuilt ook gelijk het grote risico voor de waarborging van dit kritische bedrijfsproces in. De RDWI is vooralsnog volledig afhankelijk van of de Biga Groep het SEPA-bestand tijdig en correct in het BNG-systeem zet en of zij de beveiligde toegangssleutel op tijd naar de RDWI opstuurt. Waar de RDWI bij het uitbetalen van de (bijzondere) bijstandsuitkeringen zelf de administratie verricht en veegrans uitvoert om ervoor te zorgen dat de gegevens zo actueel en correct mogelijk zijn, heeft zij die mogelijkheid bij de samenwerking met de Biga Groep vooralsnog niet. De RDWI kan ook niet zelf een SEPA-bestand genereren, omdat de juiste administratie hiervoor ontbreekt. Wel heeft de RDWI de mogelijkheid om WSW'ers eenmalig 'enkelvoudig te betalen', wat betekent dat zij handmatig de salarissen in het BNG-systeem kan zetten. Maar de RDWI heeft hier wederom wel toegang tot de administratie van de Biga Groep voor nodig.

De continuïteit van dit kritische bedrijfsproces is bij de RDWI dus niet goed gewaarborgd. De RDWI is hiervoor te sterk afhankelijk van de administratie die de Biga Groep verricht en verstuurt. Om de continuïteit van dit kritische bedrijfsproces te vergroten, zouden de Biga Groep en de RDWI er goed aan doen om nieuwe afspraken te maken over diezelfde administratie. Als er een bestand voorhanden is waarin de administratie vanuit de Biga Groep ook inzichtelijk is voor de RDWI, dan kan laatstgenoemde partij de salarissen van de WSW'ers ook handmatig laten uitbetalen via de BNG.

4.6 Uitbetalen leefgeld en vaste lasten

Als een inwoner kampt met flinke schulden kan hij zichzelf aanmelden – of via een begeleider of instantie aangemeld worden – bij de RDWI voor schuldhulpverlening. Deze inwoner komt dan terecht bij het team Schuldienstverlening (SDV), waarna een medewerker binnen dit team beoordeelt dan of de inwoner in staat is om, ondanks zijn schuldenlast, zijn vaste lasten te betalen. Als dit niet het geval is, dan wordt deze inwoner toegewezen aan een RDWI-budgetbeheerder.

In dat laatste geval staat de inwoner het beheer van zijn inkomen af aan de RDWI, die dit in eigen beheer neemt. Een budgetbeheerder van de RDWI krijgt dan de verantwoordelijkheid om van dat inkomen elke maand de vaste lasten van deze inwoner te betalen. Hier vallen onder meer diens huur, zorgkosten en schuldaflossing onder. Omdat deze betalingen prioriteit genieten, wordt ná het betalen van deze vaste lasten pas het leefgeld van de inwoner berekend en aan hem uitgekeerd. Dit leefgeld wordt wekelijks aan de desbetreffende inwoner uitgekeerd en is voor hem precies genoeg om te kunnen voorzien in het doen van zijn boodschappen en het kopen van toiletartikelen en kleding. Op deze manier wordt er door de RDWI dus heel bewust omgegaan met iemands financiën en wordt diegene geholpen in het gaandeweg aflossen van zijn schulden.

De Regisseurs Budgetbeheer bij de RDWI werken vooral met de Stratech-applicatie. Hierin staan onder meer de cliëntenkaart, de persoonsgegevens en de schuldenlijst van de inwoner vermeld. De Regisseur Budgetbeheer kan in Stratech de geldpotjes beheren en betalingen verrichten. Stratech, in beheer bij de gelijknamige softwareleverancier, draait binnen de Citrix-werkomgeving, wat betekent dat deze budgetbeheerders hun werkzaamheden ook vanuit huis kunnen verrichten.

Als de Stratech-applicatie uit de lucht is, kan de Regisseur Budgetbeheer nog wel betalingen verrichten via de Rabobank, maar heeft zij geen inzicht meer in alle extra zaken die wél in Stratech vermeld staan, zoals de geldpotjes en de persoonsgegevens. De bereikbaarheid van Stratech vormt dus het grootste risico voor de RDWI voor de continuïteit van dit kritische bedrijfsproces.

De RDWI duldt geen tolerantie van uitval voor het wekelijks uitbetalen van het leefgeld, omdat de inwoner hier slechts nipt van kan rondkomen. Hij heeft namelijk geen reservepotje tot zijn beschikking en kan dus niet geldelijk compenseren voor het niet-ontvangen van zijn leefgeld. Voor het maandelijks uitbetalen van de vaste lasten geldt er een tolerantie van uitval van maximaal 48 uur. De Regisseur Budgetbeheer heeft hier namelijk nog de mogelijkheid om met schuldeisers in gesprek te gaan. Zo kan hij aan hen communiceren dat de vaste lasten, door een storing of een crisis, op een later tijdstip betaald worden. Toch mag ook dit niet te lang duren – het moet voorkomen worden dat de inwoner hierdoor in nog grotere betalingsproblemen belandt.

4.6.1 Continuïteitsstrategie uitbetalen leefgeld en vaste lasten

De RDWI heeft vanuit de deelnemende gemeenten de taak overgedragen gekregen om schuldhelpverlening aan inwoners te verstrekken. Regisseurs Budgetbeheer van de RDWI nemen het inkomen van die desbetreffende inwoners in beheer. Hiermee betalen zij elke maand een deel van de schulden af en wordt de inwoner wekelijks van leefgeld voorzien. Binnen het schuldhelpverleningstraject hanteert de RDWI een tolerantie van uitval van maximaal 48 uur voor het betalen van de vaste lasten. De RDWI duldt geen tolerantie van uitval voor het wekelijks uitbetalen van het leefgeld.

De Regisseurs Budgetbeheer verrichten hun werkzaamheden voornamelijk in Stratech – een applicatie die beheerd wordt door Stratech en die draait op de RID-servers. Voor elke inwoner is er in Stratech een dossier aangemaakt, waarin onder meer diens cliëntenkaart, persoonsgegevens en schuldenlijst staan. Ook kan de Regisseur Budgetbeheer hierin de geldpotjes beheren en betalingen verrichten. Stratech draait bovendien binnen de Citrix-werkomgeving, wat betekent dat de Regisseur Budgetbeheer zijn werk ook vanuit huis kan doen.

Het betalen van de vaste lasten gebeurt maandelijks – vaak via automatische incasso's. Voor het wekelijks betalen van het leefgeld zijn aparte afspraken gemaakt met de inwoner – deze heeft inspraak in op welke dag hij zijn leefgeld wil ontvangen. De lijst van de inwoners wiens inkomen hij beheert kan de Regisseur Budgetbeheer ook inzien op de Stratech-applicatie. Mocht de Stratech-applicatie met een storing kampen, dan kan een Regisseur Budgetbeheer via de Rabobank ook bij het bankaccount van de inwoner om betalingen te verrichten. Hierin kan hij bijvoorbeeld ook de vorige betalingen inzien.

Toch is het uitbetalen van het leefgeld nog niet goed genoeg gewaarborgd bij de RDWI. Als de Stratech-applicatie eruit ligt, dan heeft de Regisseur Budgetbeheer geen overzicht van voor welke inwoners hij het budget beheert, hoeveel leefgeld hij over moet maken naar hen en op welke dag zij precies hun leefgeld horen te ontvangen. En dit terwijl de Regisseurs Budgetbeheer dus wél direct betalingen kunnen doen via de Rabobank. Maar, zonder toegang tot bovenstaande gegevens, is de foutmarge op deze directe betalingen een stuk hoger. De RDWI zou er daarom goed aan doen om interne afspraken te maken over het vastleggen, en het maandelijks updaten, van een back-uplijst. Hierin moeten de namen van de desbetreffende inwoners staan, de namen van de Regisseurs Budgetbeheer aan wie deze zijn toegewezen, de hoeveelheid leefgeld die de inwoners per week ontvangen, en de specifieke dagen waarop dit dient te gebeuren.

Voor het maandelijks uitbetalen van de vaste lasten geldt dat, als de Regisseurs Budgetbeheer zelf proactief contact opnemen met schuldeisers, dat zij enige coulance zullen tonen als de betalingen enkele dagen later plaatsvinden. Toch moeten de Regisseurs Budgetbeheer hier voorzichtig mee zijn – deze groep inwoners kan het zich niet veroorloven om nog veel verder in de schuldenlast te zakken.

4.7 Uitbetalen salarissen eigen werknemers

De RDWI betaalt de salarissen van haar eigen werknemers uit op de 15^e van elke maand. De afspraak is echter wel dat dit nooit op een weekenddag gebeurt. Dit betekent dat als de 15^e van die maand op een zaterdag valt, dat er dan op de 14^e wordt uitbetaald. Als de 15^e van die maand op een zondag valt, dan wordt er op de 16^e uitbetaald. Alle 'mutaties', zoals reiskostendeclaraties en urenwijzigingen, kunnen tot de 1^e van elke maand aangeleverd worden door medewerkers en leidinggevendenden. De RDWI garandeert haar werknemers dat alle mutaties die vóór de 1^e van de maand binnenkomen, meegenomen worden in de aankomende salarisuitbetaling. Conform haar eigen *Service Level Agreement* is de RDWI verantwoordelijk voor een juiste accordering en uitbetaling van de salarisadministratie.

De HR-afdeling van de RDWI keurt en verwerkt alle mutaties in een mutatiebestand in YouForce – een door Visma | Raet beheerde applicatie waarin ook alle salarisstroken en personeelsinformatie worden opgeslagen. Voor het uitbetalen van de salarissen gebruikt de RDWI Korento – een applicatie die gesynchroniseerd functioneert met YouForce. Dit betekent dat wanneer er wijzigingen plaatsvinden in YouForce, bijvoorbeeld bij het uit dienst gaan van een werknemer, dat direct ook wordt verwerkt in Korento.

Korento draait een proefrun op de 9^e of 10^e van elke maand, waarbij zij toetst of alle gegevens goed zijn ingevoerd en of de achterliggende systemen nog goed functioneren. Korento stuurt dan een e-mail naar de RDWI met de resultaten van de proefrun. Als er problemen zijn ontdekt tijdens de proefrun, dan heeft de HR-afdeling van de RDWI nog zo'n vijf dagen de tijd om deze te herstellen. Bij een geslaagde proefrun staat er in diezelfde e-mail benoemd dat de outputbestanden voor de salarissen klaarstaan. De HR-afdeling én de Unitmanager FIF geven hier dan nog hun laatste goedkeuring op. Via betalingsverwerker Equens worden de juiste geldelijke bedragen vervolgens doorgestuurd naar de bankrekeningen van de RDWI-werknemers.

Voor de continuïteit van dit kritische bedrijfsproces is de RDWI dus sterk afhankelijk van of het mutatiebestand in YouForce correct is opgebouwd en bijgehouden door haar eigen HR-afdeling en of Korento toegang heeft tot deze informatie. Hierin schuilt dan ook het grootste risico – de RDWI speelt een hele beperkte rol binnen het proces van het omzetten van de informatie in YouForce naar het daadwerkelijk uitbetalen van de salarissen door Korento. De RDWI hanteert een tolerantie van uitval van maximaal 72 uur voor dit kritische bedrijfsproces.

4.7.1 Continuïteitsstrategie uitbetalen salarissen eigen werknemers

De RDWI keert haar eigen werknemers, in principe, op de 15^e van elke maand hun salarissen uit. Gedurende de maand houdt haar eigen HR-afdeling een mutatiebestand bij in YouForce, waarin alle mutaties in de salarisadministratie worden gecontroleerd en goedgekeurd. Een externe partij, Korento, checkt deze mutaties nogmaals en betaalt, bij goedkeuring hiervan, de salarissen op de juiste datum uit aan de RDWI-werknemers. Randon deze uitbetalingsdeadline hanteert de RDWI een tolerantie van uitval van maximaal 72 uur.

Voor de continuïteit van dit gehele kritische bedrijfsproces is het cruciaal dat de applicaties YouForce én Korento naar behoren functioneren. Binnen YouForce wordt de personeelsadministratie verricht en worden alle mutaties bijgehouden, terwijl Korento gebruikt wordt om deze mutaties te checken en de salarissen uiteindelijk uit te betalen. Beide applicaties zijn toegankelijk vanuit de Citrix-werkomgeving, wat betekent dat men ook vanuit huis hiermee kan werken. YouForce en Korento “praten” met elkaar, wat betekent dat zij gebruikmaken van elkaars data en informatie. Tegelijkertijd geldt daardoor wel dat zij ook afhankelijk zijn van elkaars input. Als YouForce uit de lucht is, dan kan Korento geen toegang verkrijgen tot de data en dus geen salarissen uitbetalen. Als Korento met een storing kampt, dan kunnen de in YouForce opgebouwde salarisstroken ook niet omgezet worden in daadwerkelijke uitbetalingen.

Om dit te ondervangen is er voor beide scenario's een mogelijke oplossing. In het geval dat YouForce met een storing kampt – en Korento dus geen toegang heeft tot de juiste personeelsadministratie – is het van belang dat Korento een bestand aangeleverd krijgt waarin de administratieve data ook goed verwerkt is. De HR-afdeling van de RDWI kan dit handmatig doen: zij gebruikt dan de salarisuitbetalingen van de vorige maand als referentiekader en zet dit af tegen het mutatiebestand dat zij zelf reeds heeft opgeslagen op haar eigen N-schijf. Op deze manier ontvangen medewerkers in principe hetzelfde loon als de vorige maand en wordt er tegelijkertijd ook rekening gehouden met belangrijke wijzigingen in het personeelsbestand van de RDWI. Dit is echter alleen een werkbare optie als YouForce er langdurig uit ligt, omdat dit veel administratief werk met zich meebrengt. De Unitmanager FIF is bevoegd om hier een eindoordeel over te vellen.

Als Korento met een langdurige storing kampt, en er dus geen salarissen uitbetaald kunnen worden volgens de 'normale' route, dan kan de RDWI ertoe besluiten om zelf de salarissen handmatig uit te betalen. Via YouForce heeft zij inzage in de salarisstroken, waardoor zij zeker weet welke exacte bedragen zij aan haar werknemers moet uitkeren. Tegelijkertijd brengt ook deze variant veel administratief werk met zich mee.

Voor beide scenario's is het ontstaan van een extra administratieve last een nadelig gevolg. Om dit ondervangen kan de RDWI een "indien-nodig"-werkwijze hanteren. Hierbij communiceert de RDWI dan naar haar werknemers dat de uitbetalingen van de salarissen, bijvoorbeeld, een week later plaats zullen vinden dan normaal. Werknemers die zich dit niet kunnen veroorloven kunnen zich dan bij de HR-afdeling melden. Deze groep werknemers krijgen hun salarissen dan handmatig uitbetaald. Dit levert nog steeds wel extra administratief werk op, maar is slechts een fractie van de hoeveelheid werk die was ontstaan als dit voor álle werknemers moest worden gedaan. De verantwoordelijkheid van het hiertoe besluiten, én het toezien op de inrichting van dit alternatief, ligt bij de Unitmanager FIF.

Al met al is de continuïteit van dit kritische bedrijfsproces redelijk goed gewaarborgd. Ondanks dat de RDWI sterk afhankelijk is van twee applicaties – YouForce en Korento – voor haar salarisadministratie en -uitbetaling, kan zij, mede doordat haar eigen HR-afdeling zelf mutaties bijhoudt, in geval van nood ervoor kiezen om handmatig bepaalde stappen binnen dit bedrijfsproces te ondernemen. Zij zou het hierbij voor zichzelf kunnen vergemakkelijken door een "indien-nodig"-werkwijze te hanteren bij het doen van deze handmatige salarisuitbetalingen.

5. Cybercrisisorganisatie

5.1 Wanneer komt de cybercrisisorganisatie in actie?

De cybercrisisorganisatie van de RDWI komt niet zo maar in actie – alleen bij een crisis wordt zij geactiveerd. Maar, niet elke melding die binnenkomt is ook gelijk een daadwerkelijke (cyber)crisis. Er kan immers ook sprake zijn van een ongewenste gebeurtenis of een incident (zie 1.2). Een melding van een ongewenste gebeurtenis, een incident of een crisis kan op verschillende wijzen binnenkomen bij de RDWI:

- Een medewerker signaleert zelf een ontstaan (fysiek) probleem in het kantoorpand en informeert zijn Teamleider of Unitmanager hierover.
- De ICT-Regisseur of de Functioneel Applicatiebeheerder wordt geïnformeerd door de RID of door een andere leverancier dat er een probleem is ontstaan in de dienst(en) die zij levert.
- De Adviseur Crisisbeheersing wordt vanuit de RID door de CISO ingelicht dat er een cybercrisis op handen is. In dit geval is de RDWI overigens, conform de afspraken in het RID *Cyber Crisisplan*, verplicht om haar eigen cybercrisisorganisatie te activeren.

Ongeacht de wijze waarop een melding van een ontstaan probleem bij de RDWI binnenkomt, is het aan de betrokkene de taak om zo snel mogelijk de Manager Bedrijfsvoering hierover in te lichten. De Manager Bedrijfsvoering is, in samenspraak met de Unitmanager van het getroffen team, immers verantwoordelijk voor het beoordelen van dit ontstaan probleem – en of er sprake is van een (cyber)crisis. Ter beoordeling hiervan geldt altijd het volgende principe:

Als de continuïteit van één van de in dit Bedrijfscontinuïteitsplan Cyber beschreven kritische bedrijfsprocessen (conform *Hoofdstuk 3* en *Hoofdstuk 4*) in het geding komt en de maximale tolerantie van uitval van dit kritische bedrijfsproces dreigt te worden overschreden, dan is er sprake van een (cyber)crisis.

Aan de Manager Bedrijfsvoering is het dan, bij het besluit dat er inderdaad sprake is van een crisis, de taak om per direct de Directeur van de RDWI hierover in te lichten. In gezamenlijkheid besluiten zij dan om het Lokaal Operationeel Kernteam (L-OKT) bijeen te roepen. De Directeur van de RDWI wordt de voorzitter van dit L-OKT én vormt tevens de link naar het Algemeen Bestuur toe. De voorzitter van het Algemeen Bestuur heeft vervolgens de bevoegdheid om te besluiten of hij het Bestuurlijk Kernteam (BKT) wél of niet activeert.

5.2 Cybercrisisorganisatie: Bestuurlijk en operationeel

Crisisbestrijding is een complexe operatie waarbij veel mensen betrokken zijn en waar verschillende belangen op het spel staan. Om te garanderen dat dit zo goed mogelijk verloopt, werkt de RDWI kort vóór en tijdens de (dreigende) crisis op een andere manier dan dat zij onder normale omstandigheden doet. Het uitgangspunt is hierbij altijd dat de reguliere organisatie plaatsmaakt voor de crisisorganisatie.

Concreet betekent dit dat het Management Team (MT) zijn operationele bevoegdheden ten tijde van crisis tijdelijk overdraagt aan het L-OKT – het MT wordt vanaf dat moment ‘slechts’ geïnformeerd door het L-OKT. Op bestuurlijk niveau gebeurt iets vergelijkbaars: waar normaal gesproken het Dagelijks Bestuur (DB) en het Algemeen Bestuur (AB) de bestuurlijke laag van de RDWI vormen, is ten tijde van crisis het BKT de bestuurlijk verantwoordelijke. Het DB en het AB worden dan tijdelijk ‘slechts’ geïnformeerd door het BKT. Als de crisis voorbij is worden het L-OKT en het BKT gedeactiveerd en nemen het MT, het DB en het AB weer hun reguliere besturingsposities in.

De cybercrisisorganisatie binnen de RDWI is dus tweeledig; er is immers een bestuurlijk crisisteam – het BKT, en een operationeel crisisteam – het L-OKT. In het BKT worden de bestuurlijke besluiten genomen en wordt er overlegd met andere instanties, zoals de hulpdiensten en de RID. In het L-OKT vindt de operationele besturing van de crisis plaats en zit men dus ‘dichter op het vuur’. Het L-OKT neemt maatregelen om de crisis intern te beteugelen en ziet toe op de uitvoering van deze maatregelen. De Directeur van de RDWI is de schakel tussen beide crisisteams.

5.3 Bestuurlijk crisisteam – het Bestuurlijk Kernteam (BKT)

Ten tijde van een crisis is het Bestuurlijk Kernteam (BKT) belast met de bestuurlijke gevolgen van de (cyber)crisis te overzien en te managen. Het BKT heeft een aantal taken die zij vervult gedurende een crisis:

- Bespreken van de (mogelijk) bestuurlijke gevolgen van de crisis. Hieronder vallen ook de (mogelijke) bestuurlijke consequenties als gevolg van de acties die het L-OKT onderneemt.
- Adviseren van het bevoegd gezag en/of de RID over de verschillende scenario's en bestuurlijke vraagstukken die op tafel liggen.
- Fungeren als communicatielijn naar het DB en het AB toe.

5.3.1 Rol- en taakverdeling BKT

Het BKT bestaat uit minstens zes vaste leden, die ieder hun eigen rol vervullen in dit crisisteam. Dit zijn de:

- Voorzitter van het BKT
- Directeur van de RDWI
- Adviseur Bedrijfsvoering
- Bestuursadviseur
- Communicatieadviseur
- Notulist

Ook sluit de Burgemeester van Zeist aan indien er sprake is van een crisis waar de hulpdiensten voor benodigd zijn. De CISO en de Algemeen Directeur van de RID schuiven ook aan tafel aan als het een cybercrisis betreft.

In het overzicht op de volgende pagina staan de leden van het BKT en hun taken en verantwoordelijkheden beschreven. De leden die uit de interne organisatie afkomstig zijn, zijn dikgedrukt weergegeven.

Rol / Functie	Aanwezigheid	Taken, verantwoordelijkheden en bevoegdheden
Voorzitter BKT	Altijd aanwezig	Is voorzitter van het BKT en heeft de eindregie over de bestuurlijke crisisorganisatie. Stuur op informatie-opvraag vanuit de BKT-leden. Is normaal gesproken voorzitter van het DB. Informeert het AB én het DB. Onderhoudt nauw contact met de burgemeester van Zeist gedurende de crisis.
Directeur RDWI	Altijd aanwezig	Heeft als voorzitter van het L-OKT de eindregie over de cybercrisisorganisatie. Is bestuurlijk eindverantwoordelijk voor het L-OKT.
Adviseur Bedrijfsvoering	Altijd aanwezig	Is als Unitmanager FIF ook Manager Bedrijfsvoering in het L-OKT en daarmee verantwoordelijk voor bedrijfscontinuïteit aldaar. Heeft kennis van alle interne operationele processen. Is in het L-OKT ook de rechterhand van de voorzitter. Is tevens SOO-lid.
Bestuursadviseur	Altijd aanwezig	Is verantwoordelijk voor het adviseren van het bestuur en de directie van de RDWI.
Communicatieadviseur	Altijd aanwezig	Is verantwoordelijk voor communicatie; zowel naar de eigen medewerkers toe, als naar de inwoner en de media. Voorziet het BKT van advies met het oog op soortgelijke zaken.
Notulist	Altijd aanwezig	Noteert al dat besproken en besloten is, inclusief de afgesproken actiepunten. Is ook verantwoordelijk voor het coördineren van vergaderingen en het beheren van de agenda's van de BKT-leden.
Burgemeester Zeist	Aanwezig bij een crisis m.b.t. fysieke veiligheid	Schuift aan indien de fysieke veiligheid in het geding is als gevolg van de crisis. Is onderdeel van de Veiligheidsdriehoek en onderhoudt nauw contact met de hulpdiensten.
Directeur RID	Aanwezig bij een cybercrisis	Schuift vanuit de RID aan indien er sprake is van een cybercrisis. Is als CMT-voorzitter binnen de RID verantwoordelijk voor het leiden van dit team. Beantwoordt bestuurlijke vraagstukken die bij het BKT op tafel komen. Neemt onbeantwoorde vragen weer mee terug naar het CMT-overleg.
CISO	Aanwezig bij een cybercrisis	Schuift aan indien er sprake is van een cybercrisis. Adviseert over de impact van genomen besluiten op de informatieveiligheid bij de deelnemer. Is ook de CISO voor alle andere deelnemers én de RID.

5.4 Operationeel crisisteam – het Lokaal Operationeel Kernteam (L-OKT)

Ten tijde van een crisis is het Lokaal Operationeel Kernteam (L-OKT) belast met de interne crisisbeheersing en dus het treffen van maatregelen en voorzieningen om de impact en de gevolgen van een (cyber)crisis te mitigeren en te minimaliseren. Het L-OKT vervult de volgende taken tijdens een crisis:

- Informatie vergaren voor een zo compleet mogelijke risico- en impactanalyse.
- Beslissen over de te nemen maatregelen om de continuïteit van de kritische bedrijfsprocessen zoveel mogelijk te kunnen borgen of, waar nodig, te herstellen.
- Toewijzen van taken aan de juiste personen.
- Toezien op de uitvoering van de genomen maatregelen en de toegewezen taken.
- Verzorgen van de communicatie naar haar eigen medewerkers, de inwoners en de media toe.
- Voortdurend in contact staan met andere cruciale spelers in de crisis, zoals de de RID en andere belangrijke leveranciers.

5.4.1 Rol- en taakverdeling L-OKT

Het L-OKT bestaat uit minstens acht vaste leden uit de eigen interne organisatie, die ieder hun eigen rol vervullen in dit team. Dit zijn de:

- Voorzitter van het L-OKT
- Manager Bedrijfsvoering
- Bestuursadviseur
- Adviseur Crisisbeheersing
- Adviseur Veiligheid

- Communicatieadviseur
- ICT-regisseur
- Notulist

Afhankelijk van de aard van de crisis schuiven ook de teammanager Diensten en een SLM'er vanuit de RID en een Unitmanager of een andere interne eindverantwoordelijke aan in het L-OKT.

In het onderstaand overzicht staan de leden van het BKT en hun taken en verantwoordelijkheden beschreven. De leden die uit de interne organisatie afkomstig zijn, zijn dikgedrukt weergegeven.

Rol / Functie	Aanwezigheid	Taken, verantwoordelijkheden en bevoegdheden
Voorzitter L-OKT	Altijd aanwezig	Is Directeur van de RDWI en heeft de eindregie over de cybercrisisorganisatie. Is daarmee ook de bestuurlijke verantwoordelijke van dit team. Stuurt op informatie-opvraag vanuit de andere L-OKT-leden. Vormt ook de link met het BKT, waar zij ook in zetelt. Informeert het MT.
Manager Bedrijfsvoering	Altijd aanwezig	Is Unitmanager FIF en tevens SOO-lid. Heeft kennis van alle interne operationele processen. Is in het L-OKT verantwoordelijk voor bedrijfscontinuïteit. Deelt informatie en knelpunten met de andere L-OKT-leden. Is in het L-OKT de rechterhand van de voorzitter. Zetelt ook in het BKT.
Bestuursadviseur	Altijd aanwezig	Is verantwoordelijk voor het adviseren van het bestuur en de directie van de RDWI. Schuift vanuit deze rol ook aan in het BKT.
Adviseur Crisisbeheersing	Altijd aanwezig	Is Teamcoördinator IM. Is in het L-OKT verantwoordelijk voor de digitale veiligheid. Deelt informatie en knelpunten met de andere L-OKT-leden. Heeft kennis van het crisislandschap binnen de regionale samenwerking.
Adviseur Veiligheid	Altijd aanwezig	Is Regisseur Facilitair & Inkoop. Is in het L-OKT verantwoordelijk voor de fysieke veiligheid en heeft kennis van de fysieke veiligheidsprotocollen. Deelt informatie en knelpunten met de andere L-OKT-leden. Focust zich op de veiligheid van de medewerkers in relatie tot hun dienstverlening.
Communicatieadviseur	Altijd aanwezig	Is verantwoordelijk voor communicatie; zowel naar de eigen medewerkers toe, als naar de inwoner en de media. Voorziet het L-OKT van advies met het oog op soortgelijke zaken. Schuift vanuit deze rol ook aan in het BKT.
ICT-regisseur	Altijd aanwezig	Is in het L-OKT verantwoordelijk voor ICT. Deelt informatie en knelpunten met de andere L-OKT-leden. Is verantwoordelijk voor de uitvoer van IT-werkzaamheden indien de RID daar opdracht toe gegeven heeft. Onderhoud contact met de andere belangrijke leveranciers.
Notulist	Altijd aanwezig	Noteert al dat besproken en besloten is, inclusief de afgesproken actiepunten.
Teammanager Diensten	Aanwezig bij een cybercrisis	Schuift vanuit de RID aan indien er sprake is van een cybercrisis. Is als CMT-lid binnen de RID verantwoordelijk voor de communicatie naar de deelnemers toe. Beantwoordt vragen en geeft opdrachten mee. Neemt onbeantwoorde vragen weer mee terug naar het CMT-overleg.
SLM'er	Aanwezig bij een cybercrisis	Schuift vanuit de RID aan indien er sprake is van een cybercrisis. Ondersteunt de Teammanager Diensten in zijn rol. Is ook CMT-lid binnen de RID.
Unitmanager	Aanwezig bij een crisis die zijn team raakt	Is Unitmanager van het team dat getroffen is door de crisis. Kan daardoor extra inzicht en expertise bieden. Schuift aan op voorspraak van de voorzitter van het L-OKT.

5.5 Regionale cybercrisisrespons

De RDWI activeert dus haar eigen cybercrisisorganisatie, in de vorm van het BKT en het L-OKT, als zij getroffen wordt door een cybercrisis. Wetende dat zij één van de zeven deelnemers is die aangesloten is bij de RID, is het niet ondenkbaar dat bij een cybercrisis meerdere van deze partijen getroffen zijn door hetzelfde probleem. Elke deelnemer richt dan haar eigen BKT én L-OKT op. Vanuit dat perspectief bezien is het onmogelijk voor de Algemeen Directeur van de RID om bij alle BKT's aan te schuiven. Hetzelfde geldt ook voor de Teammanager Diensten en de SLM'er van de RID, die niet bij alle L-OKT's aanwezig kunnen zijn.

Om dit probleem te ondervangen heeft de RID in haar eigen *Cyber Crisisplan* twee scenario's geschetst waarin dit zich voor zou kunnen doen. In het door hen geschetste 'Scenario 3', waarin meerdere deelnemers getroffen zijn door een cybercrisis zonder fysieke en maatschappelijke effecten tot gevolg, schuiven de Teammanager Diensten en de SLM'er vanuit de RID juist aan bij het Strategisch Opdrachtgevers Overleg (SOO). In dit SOO zitten namelijk de Managers Bedrijfsvoering van alle deelnemers. De Manager Bedrijfsvoering moet de vragen vanuit zijn eigen L-OKT op tafel leggen tijdens dit SOO, terwijl hij ook de informatie vanuit de RID-afgevaardigden weer terug moet nemen naar zijn L-OKT. Op bestuurlijk vlak schuift de Algemeen Directeur van de RID, in plaats van de afzonderlijke BKT's, juist aan bij het Algemeen Bestuur van de RID, dat op dat moment het hoogste bestuursorgaan binnen de regionale cybercrisisrespons is. In dit overleg nemen ook onder meer de portefeuillehouders ICT, de CISO, en een Technisch Voorzitter vanuit de VRU plaats.

In het door de RID geschetste 'Scenario 4' zijn wederom meerdere deelnemers getroffen door een cybercrisis, en heeft dit wél fysieke en maatschappelijke effecten tot gevolg. Op operationeel vlak is hier weer eenzelfde belangrijke rol weggelegd voor de Managers Bedrijfsvoering van de gemeenten – zij schuiven aan bij het SOO, waar zij informatie uitwisselen met de Teammanager Diensten en de SLM'er van de RID. Op bestuurlijk niveau heeft het Algemeen Bestuur van de RID echter het stokje overgedragen aan het Bovenlokaal Crisisteam Cyber. Dit team wordt voorgezeten door de voorzitter van het Algemeen Bestuur van de RID. Hierin nemen verder ook alle burgemeesters van de deelnemers, de CISO, een Technisch Voorzitter vanuit de VRU, en de Algemeen Directeur van de RID in plaats. Dit bestuursorgaan is dan verantwoordelijk voor het overzien van de bestuurlijke gevolgen die de cybercrisis met zich meebrengt.

De precieze uitwerking van de rollen, taken en verantwoordelijkheden van alle betrokkenen binnen de regionale cybercrisisorganisatie is terug te vinden in het *Cyber Crisisplan* van de RID.

5.6 Afspraken en procedures bijeenkomen BKT en L-OKT

Tijdens het proces van crisisbesturing is het van cruciaal belang dat binnen de crisisteams alle neuzen dezelfde kant op staan – er moet eenduidigheid zijn over de manier waarop men samenwerkt, vergadert en besluiten neemt.

Het eerste uitgangspunt is dat het BKT en het L-OKT bijeenkomen op voorspraak van hun respectievelijke voorzitters (de Voorzitter van het BKT en de Directeur van de RDWI). De frequentie van bijeenkomen voor vervolgoeverleg wordt ook door diezelfde voorzitters bepaald, afgestemd op het tempo waarin de crisis zich ontwikkelt. Men dient strikte bereikbaarheidsafspraken te hanteren: degenen die aan de rollen en functies zijn toegewezen (zie 5.7) dienen zich zo snel mogelijk bereikbaar én beschikbaar te stellen om hun positie in het crisisteam in te nemen. Voor de eerste bijeenkomst van een crisisteam geldt, onder werktijden, een uiterste reactietijd van maximaal één uur. Buiten werktijden bedraagt deze reactietijd drie uur. De 'wisselspelers' dienen gedurende een crisis ook alert te zijn. Mocht een crisis zich tot een groter aantal uren strekken, dan is het aan de voorzitters van de crisisteams om vervangingsdiensten toe te wijzen.

Het tweede uitgangspunt is dat er een vast vergaderprotocol gehanteerd wordt. Voor het BKT en het L-OKT betekent dit dat zij elk overleg moeten vormgeven aan de hand van het BOB-principe, waar beeldvorming, oordeelvorming en besluitvorming centraal staan. Bij 'beeldvorming' stelt men de vragen "Wat weten we?" en "Wat weten we niet?" Bij 'oordeelvorming' bepaalt men de (ontwikkeling van de) impact van de crisis, de dilemma's die hierdoor optreden, waar nog verdere informatiewinning benodigd is en welke opties en maatregelen er op dat moment denkbaar en beschikbaar zijn. Bij 'besluitvorming' spreekt men besluiten af en wijst deze toe aan personen of instanties.

Tot slot moeten er ook afspraken gemaakt worden over de wijze waarop men bijeenkomt, welke communicatiemiddelen men hierbij gebruikt en hoe men er blijvend voor kan zorgen dat zij de juiste informatie binnen krijgt. Bijeenkomen op eenzelfde fysieke locatie heeft logischerwijs de voorkeur – hiervoor zijn, indien het RDWI-kantoorpand in Zeist onbereikbaar of niet-beschikbaar zijn, twee opties mogelijk. De RDWI heeft immers afspraken met de gemeente Zeist en de gemeente Wijk bij Duurstede afspraken dat zij hun gemeentehuis als uitwijklocatie kunnen gebruiken. De voorkeur gaat hierbij uit naar het gemeentehuis in Zeist. De burgemeester van Zeist schuift immers soms aan bij het BKT en de gemeente Zeist is ook geen onderdeel van de RDWI, waardoor zij mogelijk niet getroffen zijn door een cybercrisis die de RDWI, en andere RID-deelnemers, wél treft. Mochten deze opties ook niet-beschikbaar zijn, dan is het aan de voorzitter van diens crisisteam om een andere uitwijklocatie te bepalen en te regelen. Als dit óók geen optie is, of als een aantal crisisteamleden niet (tijdig) fysiek aanwezig kunnen zijn, dan dient men te overleggen via het hiervoor aangemaakte Microsoft Teams-kanaal.

De Bestuursadviseur bepaalt de vormgeving van de bestuurlijke communicatie gedurende een crisis, terwijl de Communicatieadviseur in het operationele crisisteam verantwoordelijk is voor de interne communicatie naar de medewerkers van de interne organisatie. Zij dienen hierover onderling afstemming te regelen. Een verdere uitwerking hiervan is te vinden in *Hoofdstuk 6*.

5.7 Toewijzing namen aan rollen BKT en L-OKT

Voor elke rol in de twee crisisteams moeten ook twee specifieke personen toegewezen worden. De eerstgenoemde persoon vervult die rol, de ander fungeert als stand-in. Als de crisis voor een langere periode aanhoudt verandert deze rolverdeling in een aflossingsschema – de twee aangewezen personen nemen dan om de zoveel tijd het stokje over van de ander.

In *Bijlage 1* staat de naam- en rolverdeling voor het BKT en het L-OKT vermeld.

6. Communicatie

6.1 Communicatie als cruciaal component cybercrisisbeheersing

Juist in tijden van crisis wordt het belang van goede communicatie nóg duidelijker. De Veiligheidsregio Utrecht (VRU) benoemt in haar *Regionaal Crisisplan* dat risico- en crisiscommunicatie een cruciaal onderdeel vormen van crisisbeheersing.

Volgens de VRU is crisiscommunicatie "het verzamelen, verwerken en verspreiden van informatie die van belang is om een incident of crisis aan te pakken, met als doel: informatievoorziening, schadebeperking en betekenisgeving³."

De VRU koppelt hier een aantal belangrijke randvoorwaarden aan. Zo moeten betrokken partners in onderlinge afstemming én conform hun verantwoordelijkheden en lijnen alle benodigde informatie in hun crisisteams delen. Ook moet men bij incidenten en crises zoveel mogelijk gebruikmaken van bestaande kanalen en communicatiemiddelen. Voor de RDWI betekent dit concreet dat er een vastgesteld en helder beeld is van met welke partijen er gecommuniceerd moet worden, hoe deze communicatieboodschappen vormgegeven moeten worden, welke middelen van communicatie er (per doelgroep) gebruikt moeten worden, en welke personen welke rollen, taken en bevoegdheden toebedeeld krijgen.

6.1.1 Crisiscommunicatie – Wanneer start je hiermee?

Tijdens een crisis is het van belang om als organisatie zijnde de regie zoveel mogelijk in eigen handen te houden. Volgens het 'stealing thunder'-principe kan het snel en zelf naar buiten treden met berichtgeving, voordat werknemers, inwoners en media met vragen komen te zitten, ertoe leiden dat je als organisatie de regie over de initiële boodschap behoudt en dat je direct signaleert dat je een betrouwbare bron bent die bovendien transparant handelt. Het startsignaal voor het doen van crisiscommunicatie wordt altijd vanuit de crisisteams binnen de cybercrisisorganisatie gegeven.

6.1.2 Crisiscommunicatie – Tot wie richt je je?

De aard en de inhoud van de crisiscommunicatie moet afgestemd worden op de doelgroepen waartoe deze gericht is. Het *Communicatieplan Cybercrisis*⁴ van de RDWI bevat een opsomming van het brede scala aan doelgroepen waar hierbij aan gedacht kan en moet worden. Ook staat hierin benoemd via welk medium zij op een juiste wijze kunnen worden geïnformeerd. Deze doelgroepen zijn:

- Eigen medewerkers
- Het Algemeen Bestuur (AB) en het Dagelijks Bestuur (DB)
- Communicatieadviseurs van de RID-gemeenten plus de gemeente Zeist
- Inwoners van de vijf deelnemende gemeenten
- Leveranciers
- De media

³ Regionaal Crisisplan Veiligheidsregio Utrecht 2024-2027

⁴ Communicatieplan Cybercrisis RDWI

6.1.3 Crisiscommunicatie – Wat communiceer je?

In het *Communicatieplan Cybercrisis* worden drie richtlijnen benoemd waar rekening mee gehouden dient te worden bij het verspreiden van communicatie:

- Bedenk hoe beelden en visualisaties, zoals *infographics*, kunnen bijdragen aan betere duiding van ingewikkelde technische materie.
- Houd rekening met communicatie op B1-niveau, zodat inwoners op een begrijpelijke manier geïnformeerd worden.
- Breng zoveel mogelijk zelf nieuws naar buiten en deel vooral wat je al wél weet.

In *Bijlage 1* van het *Communicatieplan Cybercrisis* zijn voorbeelden en formats van communicatieberichten opgenomen die tijdens een cybercrisis gebruikt kunnen worden.

6.1.4 Crisiscommunicatie – Rollen en verantwoordelijkheden

In zowel het BKT als het L-OKT is de communicatie geborgd – in het BKT neemt een Bestuursadviseur plaats, in het L-OKT zit een Communicatieadviseur. Dit betekent dat hun input binnen deze crisisteams op het gebied van communicatie leidend is. In het BKT zet de Bestuursadviseur de grote strategische lijnen voor de communicatie uit en overziet zij de bestuurlijke consequenties ervan. De Communicatieadviseur in het L-OKT focust zich op de uitvoering. De Bestuursadviseur en de Communicatieadviseur moeten hierin onderlinge afstemmingen zoeken. Hierbij worden zij ondersteunt door andere communicatiemedewerkers, die zich onder andere richten op *social mediawatching* en -analyse, perscontact en administratieve en fysieke ondersteuning.

Voor andere crisisleiden én leden van de interne organisatie is er dus ook een rol weggelegd op dit onderwerp. Hieronder is er, conform het eigen *Communicatieplan Cybercrisis*, een opsomming van deze rollen en verantwoordelijkheden weergegeven. De namen van de personen die aan deze rollen zijn toegewezen, zijn terug te vinden in datzelfde *Communicatieplan Cybercrisis*.

Rol / Functie	Taken en verantwoordelijkheden
Directeur RDWI	Is eindverantwoordelijke voor al dat gecommuniceerd wordt.
Bestuursadviseur	Overziet de bestuurlijke consequenties van de communicatie. Is perswoordvoerder bij crisissituaties. Zoekt afstemming met de Communicatieadviseur.
Communicatieadviseur	Bepaalt de interne communicatie naar medewerkers toe. Zoekt hierin afstemming met de Bestuursadviseur.
Perscontact	Beheert aanvragen voor interviews, noteert vragen vanuit de pers en maakt gevalideerde informatie (telefonisch) over.
Media-analist	Monitort berichtgeving op social media en websites over de crisissituatie.
Redacteur Social Media, Pers en Website	Schrijft en publiceert updates op sociale media, via de pers en op de website.
Overige Unitmanagers en Teamleiders	Houden hun teams op de hoogte waar mogelijk. Zorgen voor een continue stroom van informatie-opgaling naar de crisisteams toe.
Verantwoordelijk Infolijn of Contact Center	Zorgt voor de oprichting en opvolging van een infolijn of een Contact Center
Administratieve en fysieke ondersteuning	Voorziet in de benodigde technische en administratieve ondersteuning, zoals het verschaffen van catering, een draadloos netwerk en printers.

6.1.5 Crisiscommunicatie – Communicatiemiddelen

Het communicatiemiddel dat gebruikt wordt om te communiceren gedurende een crisis is van groot belang – het moet een medium zijn waarmee zo veel mogelijk personen binnen de bedoelde doelgroep(en) bereikt wordt. Een andere belangrijke afweging voor het communicatiemiddel dat gebruikt gaat worden is of deze wel toegankelijk is. Afhankelijk van het soort crisis waar de gemeente door is getroffen kan dit namelijk variëren. Als er bijvoorbeeld sprake is van een grootschalige IT-storing op het interne netwerk van de gemeentelijke organisatie, dan is communiceren via het Intranet geen goede optie.

Het *Communicatieplan Cybercrisis* benoemt dat voor interne communicatie onder meer het Intranet, Microsoft Teams, e-mail en WhatsApp passende communicatiemiddelen zijn. Voor communicatie naar buitenaf toe behoren onder meer berichtgeving op de RDWI-website en *social media* en het contacteren van de pers en het versturen van brieven tot de opties.

In het *Communicatieplan Cybercrisis* is uitgebreid toegelicht welke communicatiemiddelen beschikbaar zijn, zowel online als offline, hun reikwijdte, voor welke doelgroep zij bestemd zijn en wiens taak het is om deze communicatielijn te onderhouden.

7. Décharge – Terug naar normaal

7.1 Doel déchargeproces

Op een gegeven moment is de crisis onder controle en zijn de gevolgen ervan gemitigeerd. Het doel van het déchargeproces is om op een veilige en gecontroleerde wijze af te schalen in de opgezette crisisorganisatie en een zorgvuldige overdracht naar de hierop volgende herstel- en nafase. Bij dit proces ligt de focus op het weer opstarten en borgen van de kritische bedrijfsprocessen en het inrichten van een evaluatieproces, om zo ook te kunnen leren van wat er zich heeft afgespeeld.

7.2 Sein start déchargeproces

Als er vanuit de interne organisatie, of vanuit andere stakeholders of getroffen en, steeds meer signalen binnenkomen dat de crisis onder controle is, dan is het aan de voorzitters van de crisisteams de taak om een besluit te nemen over óf het déchargeproces opgestart kan worden. Dit doen zij altijd in gezamenlijkheid – het kan namelijk voorkomen dat de bestuurlijke crisisbeheersing gereed lijkt, maar dat er op operationeel vlak nog enkele crisisbeheersingsacties nodig zijn.

7.3 Communicatie start déchargeproces

Als er gestart wordt met het déchargeproces, dan moet dit expliciet aan de relevante stakeholders en doelgroepen gecommuniceerd te worden. Vanuit het oogpunt van crisiscommunicatie bezien is het raadzaam om na de crisis het crisiscommunicatieproces nog even door te laten lopen. Er kunnen namelijk nog belangrijke communicatie- en informatiebehoeften spelen bij andere betrokkenen en getroffen en.

De in de crisisteams zittende Bestuursadviseur en Communicatieadviseur zijn hier dan hoofdelijk verantwoordelijk voor. Zij stellen, in onderling overleg met elkaar én het team Communicatie, communiqués op die gebruikt worden in de communicatie naar buitenaf toe. Richtlijnen en formats hiervoor zijn te vinden in het *Communicatieplan Cybercrisis*. Vanuit het BKT en het L-OKT worden één of twee aanspreekpunten aangewezen. Zij zijn dan te benaderen door medewerkers, inwoners of andere betrokkenen en beantwoorden de vragen en de zorgen waar diegenen dan nog mee zitten. Als het aanspreekpunt geen passend antwoord op een vraag of een verzoek weet of heeft, dan legt hij dit terug 'op tafel' bij zijn crisisteam.

7.4 Evaluatie

Een belangrijk onderdeel van het déchargeproces is het evalueren van de oorzaken, het verloop en de gevolgen van de voorbij crisis. Voortschrijdend inzicht hierin biedt namelijk kansen voor de organisatie om verbeteringen in gang te zetten. Deze evaluatie vindt op twee vlakken plaats – zowel inhoudelijk, als op communicatief vlak.

7.4.1 Inhoudelijke evaluatie

Binnen het BKT wordt allereerst een discussie gevoerd over welke zaken en bedrijfsprocessen een inhoudelijke evaluatie behoeven. Alle items die geëvalueerd moeten worden, worden onderverdeeld in 'kernthema's' – een aanpak die vergelijkbaar is met hoe de Veiligheidsregio Utrecht haar 'nafase' ook inricht⁵. Elk kernthema wordt opgepakt door een daarvoor opgericht projectteam, met aan het hoofd ervan een projectleider. Het BKT is verantwoordelijk voor de benoeming van deze projectleiders.

Elk van deze projectleiders stelt voor zijn kernthema een projectplan op, wat onder meer een planning, een schatting van de capaciteit en de middelen, en een verwachte kostenopgave bevat. De projectleider maakt afspraken met het BKT over de frequentie en de wijze waarop hij rapporteert over de voortgang van het projectteam.

Voor elk projectteam geldt dat zij op zijn minst de volgende drie doelen heeft:

- Het herstellen van de bedrijfscontinuïteit binnen zijn kernthema.
- Het evalueren van datgene wat er zich binnen zijn kernthema tijdens de crisis heeft afgespeeld.
- Het voorkomen van nieuwe en vergelijkbare situaties door adviezen af te geven over mogelijke nieuwe maatregelen, richtlijnen en implementaties.

7.4.2 Evaluatie communicatieproces

Het *Communicatieplan Cybercrisis* benoemt dat het belangrijk is om de wijze van communiceren naar alle betrokkenen en doelgroepen ook te evalueren. Op basis van verkregen inzichten vanuit deze crisis kan de aanpak, met het oog op toekomstige crisisbeheersing, aangescherpt worden.

In het *Communicatieplan Cybercrisis* worden de volgende vragen benoemd die gebruikt kunnen worden bij deze evaluatie:

- Wat heeft er goed of minder goed gewerkt? Hoe kun je dat in de toekomst verbeteren?
- Werden de juiste doelgroepen bereikt, hebben ze de boodschap bergrepen en op de juiste manier gereageerd?
- Zijn bijkomende middelen, tools of expertise nodig?
- Moeten bepaalde processen voor crisiscommunicatie vaker getest worden of beter afgesproken worden?

7.5 Debriefing

Het is ook raadzaam om na afloop van de crisis een fysieke bijeenkomst te organiseren ter debriefing. Door medewerkers vanuit alle hoeken van de eigen organisatie hierbij te betrekken creëer je als crisisorganisatie zijnde meer interactie. Dit leidt tot een meer gedragen evaluatie, bredere *lessons learned* voor de toekomst en, mogelijk, ook tot het een aanpassing van huidige plannen en protocollen.

⁵ Plan van Aanpak Overdrachtsdocument Nafase – Landelijk Netwerk Bevolkingszorg. CrisisUtrecht

B1. Overzicht crisisteamleden

B1.1 Lijst BKT-leden

Per 1 november 2025 zijn de volgende personen toegewezen als BKT-lid of als 'wisselspeler' hiervoor. Dikgedrukt zijn degenen vermeld die vanuit de eigen interne organisatie worden aangeleverd.

Rol / Functie in het BKT	Naam	Wisselspeler / Loco
Voorzitter BKT	Walter van Dijk	Julie d'Hondt
Directeur RDWI	Bernice Ruiter	Josje Hoppenbrouwers
Adviseur Bedrijfsvoering	Cas van der Eem	John van der Vorst
Bestuursadviseur	Josje Hoppenbrouwers	
Communicatieadviseur	Jellinka Kuik	Jenna Boutens
Notulist	Arne Hoekerd	André Hoogendoorn
Burgemeester Zeist	Joyce Langenacker	
Directeur RID	Robert Groenendijk	
CISO	Vincent van Bommel	

B1.2 Lijst L-OKT-leden

Per 1 november 2025 zijn de volgende personen toegewezen als L-OKT-lid of als 'wisselspeler' hiervoor. Dikgedrukt zijn degenen vermeld die vanuit de eigen interne organisatie worden aangeleverd.

Rol / Functie in het L-OKT	Naam	Wisselspeler / Loco
Directeur RDWI	Bernice Ruiter	Josje Hoppenbrouwers
Manager Bedrijfsvoering	Cas van der Eem	John van der Vorst
Bestuursadviseur	Josje Hoppenbrouwers	
Adviseur Crisisbeheersing	Marina van Staden	Saskia Schram
Adviseur Veiligheid	Brenda Krelekamp	Ron Dirksen
Communicatieadviseur	Jellinka Kuik	Jenna Boutens
ICT-regisseur	Sally Hermsen	Patrick Dijkstra
Notulist	Arne Hoekerd	André Hoogendoorn
Teammanager Diensten RID	Marc van Uunen	Edwin Wolkorte
Service Level Manager RID	Lamees Sadek	Ravi Sharma

B2. Contactgegevens crisisteamleden

B2.1 Lijst contactgegevens BKT-leden

Rol / Functie	Naam	Telefoonnummer	E-mailadres
Voorzitter BKT	Walter van Dijk	06-22920368	w.van.dijk@zeist.nl
Voorzitter BKT (2)	Julie d'Hondt	06-18898274	j.dhondt@bunnik.nl
Directeur RDWI	Bernice Ruiter	06-34497472	b.ruiter@rsdkrh.nl
Directeur RDWI (2)	Josje Hoppenbrouwers	06-51756037	j.hoppenbrouwers@rsdkrh.nl
Adviseur Bedrijfsvoering	Cas van der Eem	06-54218676	c.vandereem@rsdkrh.nl
Adviseur Bedrijfsvoering (2)	John van der Vorst	06-46052794	j.vandervorst@rsdkrh.nl
Bestuursadviseur	Josje Hoppenbrouwers	06-51756037	j.hoppenbrouwers@rsdkrh.nl
Bestuursadviseur (2)			
Communicatieadviseur	Jellinka Kuik	06-48864574	j.kuik@rsdkrh.nl
Communicatieadviseur (2)	Jenna Boutens	06-43438568	j.boutens@rsdkrh.nl
Notulist	Arne Hoekerd	06-34249580	a.hoekerd@rsdkrh.nl
Notulist (2)	André Hoogendoorn	06-39107676	a.hoogendoorn@rsdkrh.nl
Burgemeester Zeist	Joyce Langenacker		
Locoburgemeester Zeist			
Algemeen Directeur RID	Robert Groenendijk		r.groenendijk@rid-utrecht.nl
Algemeen Directeur RID (2)			
CISO	Vincent van Bommel		v.vanbommel@rid-utrecht.nl
CISO (2)			

B2.2 Lijst contactgegevens L-OKT-leden

Rol / Functie	Naam	Telefoonnummer	E-mailadres
Voorzitter L-OKT	Bernice Ruiter	06-34497472	b.ruiter@rsdkrh.nl
Voorzitter L-OKT (2)	Josje Hoppenbrouwers	06-51756037	j.hoppenbrouwers@rsdkrh.nl
Manager Bedrijfsvoering	Cas van der Eem	06-54218676	c.vandereem@rsdkrh.nl
Manager Bedrijfsvoering (2)	John van der Vorst	06-46052794	j.vandervorst@rsdkrh.nl
Bestuursadviseur	Josje Hoppenbrouwers	06-51756037	j.hoppenbrouwers@rsdkrh.nl
Bestuursadviseur (2)			
Adviseur Crisisbeheersing	Marina van Staden	06-51627592	m.vanstaden@rsdkrh.nl
Adviseur Crisisbeheersing (2)	Saskia Schram		s.schram@rsdkrh.nl
Adviseur Veiligheid	Brenda Krelekamp	06-48108175	b.krelekamp@rsdkrh.nl
Adviseur Veiligheid (2)	Ron Dirksen	06-46407450	r.dirksen@rsdkrh.nl
Communicatieadviseur	Jellinka Kuik	06-48864574	j.kuik@rsdkrh.nl
Communicatieadviseur (2)	Jenna Boutens	06-43438568	j.boutens@rsdkrh.nl
ICT-regisseur	Sally Hermsen	06-57491190	s.hermesen@rsdkrh.nl
ICT-regisseur (2)	Patrick Dijkstra	06-42329949	p.dijkstra@rsdkrh.nl
Notulist	Arne Hoekerd	06-34249580	a.hoekerd@rsdkrh.nl
Notulist (2)	André Hoogendoorn	06-39107676	a.hoogendoorn@rsdkrh.nl
RID Teamman. Diensten	Marc van Uunen	06-28151824	m.vanuunen@rid-utrecht.nl
RID Teamman. Diensten (2)	Edwin Wolkorte		e.wolkorte@rid-utrecht.nl
RID SLM'er	Lamees Sadek		l.sadek@rid-utrecht.nl
RID SLM'er (2)	Ravi Sharma		r.sharma@rid-utrecht.nl

B3. Contactgegevens leveranciers en andere partijen

B3.1 Lijst contactgegevens externe leveranciers

Leverancier	Contactpersoon	Telefoonnummer	E-mailadres
Biga Groep	Hans van Driel	030-8503200	hvandriel@bigagroep.nl
Centric	Paul Bruin	0182-345701	info.pss@centric.eu
Korento	Marleen Backer Dirks	06-43615783	m.backerdirks@rsdkrh.nl
Shift 2	Katja Dorder	06-51913706	Katja.dorder@shift2.nl
Stratech	Erik Mijnheer	06-51694357	e.mijnheer@stratech.nl
Visma Raet	Marleen Backer Dirks	06-43615783	m.backerdirks@rsdkrh.nl
YouForce	Marleen Backer Dirks	06-43615783	m.backerdirks@rsdkrh.nl

B3.2 Lijst contactgegevens andere partijen

Partij	Contactpersoon	Telefoonnummer	E-mailadres
BNG	<i>Klantenservice</i>	070-3750555	klantenservice@bngbank.nl
Gemeente Wijk bij Duurst.			
Gemeente Zeist			
RID	Heinrich Boldewijn	088-0310487	h.boldewijn@rid-utrecht.nl

B4. Samenvatting

B4.1 Schematisch overzicht kritische bedrijfsprocessen

Kritisch bedrijfsproces	Tolerantie van uitval	Grootste risico's	Waarborging
Bereikbaar zijn voor indienen aanvragen	72 uur	Afhankelijkheid van RID, Snelbalie en eigen pand	Drie wijzen bereikbaarheid, extra telefonisten, uitwijklocatie afgesproken
Bereikbaar zijn voor contact met inwoners	Geen	Wegvallen communicatie leidt tot chaos	E-mail en bellen vanuit huis, extra telefonisten, uitwijklocatie afgesproken
Uitbetalen van bijstandsuitkeringen	Geen	Strakke deadlines, sterk afhankelijk van Suite	Veel checks, wel handmatig betalen, geen back-ups, hoge foutmarge
Uitbetalen van bijzondere bijstandsuitkeringen	Geen (struct.k) 48 uur (inci.k)	Strakke deadlines, sterk afhankelijk van Suite	Veel checks, wel handmatig betalen, geen back-ups, wel schuldeisers bellen
Verstrekken van broodnoodvoorschot	Geen	Fysieke bereikbaarheid RDWI is buiten eigen macht	Uitwijklocatie afgesproken, wel nog cash paraat hebben aldaar
Uitbetalen van salarissen van WSW'ers	Geen	Strakke deadlines, sterk afhankelijk van Biga Groep	Wel handmatig betalen, geen back-up, hoge foutmarge
Uitbetalen van leefgeld en vaste lasten	Geen (leefgeld) 48 uur (vast.l)	Sterk afhankelijk van Stratech	Wel betalen via Rabobank, geen lijst persoonsgegevens, schuldeisers bellen
Uitbetalen van salarissen van eigen werknemers	72 uur	Afhankelijk van YouForce, Korento en mutatiebestand	Strakke procedures, handmatig betalen, HR checkt mutatiebestand