Risicoanalyse van toepassing op het rampenplan

1. Waarschuwing

De minimale normen van de Kruispuntbank van de Sociale Zekerheid preciseren dat de OCMW's *"aan de hand van een gezamenlijke methode, aanvaard door de werkgroep "Informatieveiligheid" of elke andere methodologie die rekening houdt met de hierin beschreven principes een risicoanalyse moeten uitvoeren teneinde de uitwerking van een continuïteitsplan mogelijk te maken.*"

De risicoanalyse dient om een inventaris op te maken van de vermoedelijke risico's. Het is de taak van de veiligheidsconsulent om die te evalueren, het resultaat van zijn risicoanalyse voor te leggen aan de secretaris en het resultaat van hun gemeenschappelijke analyses voor te leggen aan de Raad voor Maatschappelijk Welzijn, die vervolgens zal beslissen die al dan niet te goed te keuren. Die inventaris dient als basis voor de uitwerking van het driejaarlijks veiligheidsplan, omdat de veiligheidsconsulent daarin een overzicht geeft van alle acties die moeten worden ondernomen om de door de Raad voor Maatschappelijke Welzijn gekozen risico's te dekken. Tot slot ondersteunt de risicoanalyse ook het continuïteits- of rampenplan.
Zodra de risico's veranderen, moet de risicoanalyse worden bijgewerkt: nieuwe risico's (nieuwe servers, nieuwe informatica, nieuw gebouw, nieuwe organisatie), risico's die verdwijnen (papierversnipperaar die wordt weggedaan, oud fotokopieertoestel dat uit dienst wordt genomen, enz.).

Opgelet: het is niet omdat uit de risicoanalyse blijkt dat er X risico's moeten worden ingeperkt dat die X risico's in een jaar tijd moeten worden behandeld. De prioritaire risico's komen als eerste aan bod en moeten zo snel mogelijk worden weggewerkt. De andere risico's dienen in het driejaarlijks veiligheidsplan te worden opgenomen.

De analyse moet noch naar de POD MI, noch naar het Sectoraal comité van de sociale zekerheid worden opgestuurd. Ze blijft eigendom van het OCMW, dat die ter gelegenheid van een eventuele audit kan voorleggen.
Dat document mag niet verward worden met de jaarlijkse vragenlijst die de POD MI in naam van het Sectoraal comité van de sociale zekerheid opstuurt.
Aan de hand van de jaarlijkse vragenlijst kan het Sectoraal comité van de sociale zekerheid de evolutie evalueren van de manier waarop de minimale normen binnen de OCMW's worden toegepast.

De hier voorgestelde risicoanalyse heeft geen verplicht karakter. Iedere OCMW-veiligheidsconsulent is vrij om zijn eigen methodologie te kiezen, voor zover die beantwoordt aan de minimale norm. Bedoeling van de hier voorgestelde analyse is echter de OCMW's een methodologie aan te reiken die eenvoudig is opgevat en makkelijk kan worden toegepast. De Kruispuntbank van de Sociale Zekerheid heeft die methodologie herzien en erkend.

2. Kenmerken van de voorgestelde methodologie.

Deze methodologie kenmerkt zich door volgende bijzonderheden: ze is niet volledig in de technische betekenis van het woord maar volstaat voor de OCMW's omdat haar reikwijdte beperkt is tot de sociale gegevens die ofwel op papier ofwel digitaal (informatica) bewaard worden.
De analyse heeft enkel betrekking op de diensten die sociale gegevens behandelen die via de KBSZ worden beheerd:

- het RMI,
- de wet 65,
- de boekhouding (de boekhoudgegevens worden wel niet via de KBSZ beheerd, maar maken gebruik van sociale gegevens die afkomstig zijn uit de sociale software voor de toekenning van het RMI),
- andere activiteiten die behandeling en opslag van sociale gegevens vereisen.

Er wordt naar gestreefd de zaken zo eenvoudig en praktisch mogelijk te houden, omdat de risicoanalyse het rampen- of continuïteitsplan voorafgaat en helpt uit

te werken. Ze berust op de principes van de minimale veiligheidsnormen van de KBSZ en op de basisveiligheidsprincipes: vertrouwelijkheid, integriteit, beschikbaarheid, auditabiliteit (de mogelijkheid om het al dan niet bestaan van een zaak, een gebeurtenis te controleren).

Omdat elk OCMW het beheer van het RMI, de wet 65 en andere wettelijke taken op zijn eigen manier organiseert, is er geen activiteitenlijst uitgewerkt. Het is de taak van iedere veiligheidsconsulent om de hierboven aangehaalde principes toe te passen, ter herinnering, de risico's die gekoppeld zijn aan de toegang tot sociale gegevens.

3. Tot wie richt deze risicoanalyse zich?

Deze risicoanalyse richt zich tot de veiligheidsconsulenten die ze in samenwerking met hun secretaris zullen uitvoeren. Ze zal vervolgens ter goedkeuring worden voorgelegd aan de Raad voor Maatschappelijk Welzijn.

4. Principe van de risicoanalyse.

Het principe van de risicoanalyse bestaat erin te bepalen welke diensten van het OCMW het meest kritiek of kwetsbaar[1] zijn in geval van ramp of incident met gevolgen voor die diensten. Het doel van deze analyse is te kunnen anticiperen op de gevolgen van de risico's die door de veiligheidsconsulent, de secretaris – de Voorzitter – informatici en dienstverantwoordelijken werden geëvalueerd, en dat door te voorzien in corrigerende acties wanneer het risico niet aanvaardbaar is.

Laten we dat principe aan de hand van een concreet voorbeeld illustreren.
Indien een OCMW een reëel risico loopt om getroffen te worden door een overstroming en de door die overstroming aangerichte schade dat OCMW

[1] Kwetsbare diensten: diensten waarvan de werking beïnvloed is of kan worden.

gedurende drie weken zou verhinderen zijn wettelijke taken uit te voeren, kan het OCMW op **drie** manieren reageren:

1. het risico is **aanvaardbaar** en er wordt geen enkele actie ondernomen,
2. het risico is **voor sommige diensten** niet aanvaardbaar en het OCMW neemt vanaf nu maatregelen opdat het zijn kernactiviteiten opnieuw kan opstarten binnen de periode die het zichzelf oplegt (24 u, 48 u, 72 u of meer),
3. het OCMW vindt dat het risico **voor geen enkele dienst aanvaardbaar is** en neemt de nodige maatregelen opdat het al zijn activiteiten opnieuw kan opstarten binnen de periode die het zichzelf oplegt (24 u, 48 u, 72 u of meer).

Het spreekt voor zich dat de veiligheidsconsulent eventueel al over bepaalde hulpmiddelen kan beschikken: behoefteninventaris om opnieuw op te starten (lokaal, meubilair, informatica, verbindingen), veiligheidsbeleid, externe bijstand, back-ups die gemaakt en bewaard worden door een bedrijf dat zich buiten de gebouwen van het OCMW bevindt, enz.

5. Wat is een risico en wat is een aanvaardbaar risico?

a) Het risico.

Een risico is de waarschijnlijkheid dat er zich een gevaar voordoet waarbij er schade optreedt die het OCMW geheel of gedeeltelijk verhindert te functioneren.

Sommige risico's zijn gekend, andere minder. De mogelijkheid dat het risico zich voordoet, mag evenwel onderschat noch overschat worden. De veiligheidsconsulent kan daartoe informatie inwinnen bij:

- de politie voor risico op diefstal, agressie, vandalisme of andere,
- verzekeringsmaatschappijen die over nuttige statistieken en informatie beschikken inzake brand, overstroming, agressie of andere,
- het KMI (Koninklijk Meteorologisch Instituut) dat de overstromingsrisicozones kent,

- sommige beroepsverenigingen voor informaticarisico's (BELCLIV, SANS,…).

Uit dit alles vloeit voort dat het nulrisico onbestaande is. Indien er in de streek al vier jaar geen diefstal werd gepleegd, betekent dat natuurlijk niet dat het OCMW niet het slachtoffer van diefstal zal worden, a fortiori indien er geen enkele voorzorgsmaatregel genomen wordt.

b) Het aanvaardbaar risico.

Een aanvaardbaar risico is een risico waaraan het OCMW het hoofd kan bieden zonder specifieke veiligheidsmaatregelen te treffen.
Voorbeeld: wanneer het OCMW oordeelt dat het uitvallen van zijn server een aanvaardbaar risico is, dan wil dat zeggen dat het van mening is dat die server kan worden vervangen en geconfigureerd binnen een periode die zijn inschatting niet overschrijdt (24 u, 48 u, 72 u of meer) en zonder dat daarbij de goede werking van zijn diensten gehinderd wordt.

Er kan een vrij eenvoudige methodologie worden toegepast om de risico's te meten en er het gepaste belang aan toe te kennen.

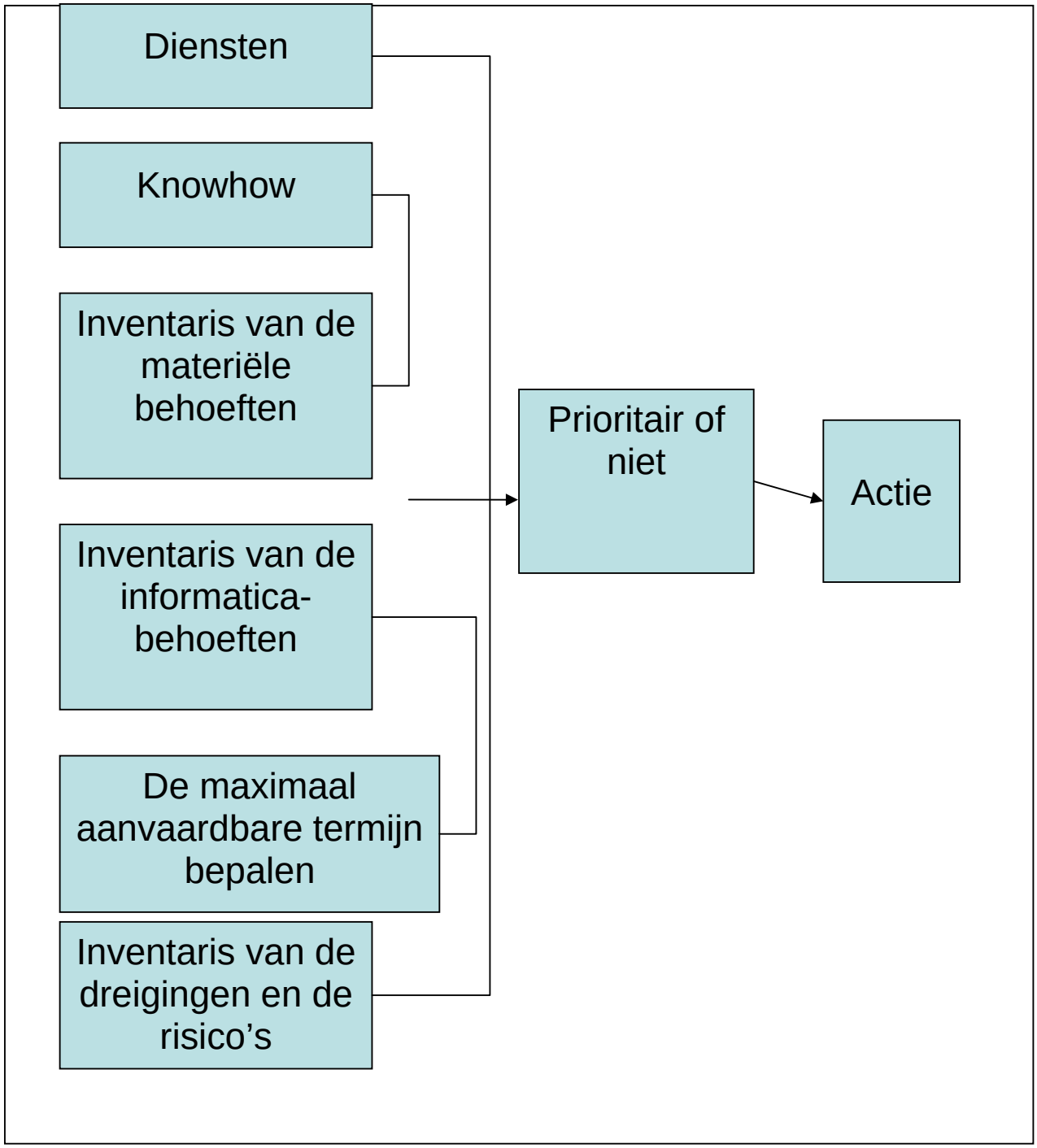
1. Een OCMW verricht veel gevarieerde activiteiten. Die liggen aan de basis van de bestaansreden van het OCMW en van zijn werking.
2 De uitvoering van die activiteiten vergt bijgevolg knowhow, personeel en materieel.
3. Daartoe moet er met computerapparatuur- en programmatuur worden gewerkt.
4. De veiligheidsconsulent bepaalt in samenwerking met de secretaris/Voorzitter en eventueel andere personen (informaticus, consulenten, enz.) de maximaal aanvaardbare onbeschikbaarheidsduur, m.a.w. de maximumperiode tijdens welke het OCMW, de dienst, de cel of sommige personeelsleden onwerkzaam kunnen blijven. Ze stellen die maximaal aanvaardbare onbeschikbaarheidsduur voor aan de Raad voor Maatschappelijk Welzijn en/of aan het Bestendig Bureau. De Raad voor

Maatschappelijk Welzijn of het Bestendig Bureau zal dan een beslissing nemen.

5. Niet al die activiteiten zijn immers onderhevig aan hetzelfde risico. Een schuldbemiddeling is eventueel een minder riskante activiteit en heeft dus een lagere prioriteit dan de uitbetaling van het leefloon.
6. Niet alle OCMW-diensten hebben dezelfde prioriteit. Het komt de Raad voor Maatschappelijk Welzijn en/of het Bestendig Bureau toe om de prioriteiten voor de heropstart te bepalen.
7. De conclusie van de risicoanalyse moet toelaten om corrigerende acties te ondernemen, zodat het OCMW zijn dienstverlening binnen de vooropgestelde termijnen kan blijven garanderen.

Op basis van deze studie kan de veiligheidsconsulent actieprioriteiten definiëren die hij dan opneemt in zijn driejaarlijkse veiligheidsplan.

6. LOGICA VAN DE RISICOANALYSE



Diensten

6A. Diensten

Alle Belgische OCMW's hebben dezelfde doelstellingen maar zijn naargelang hun capaciteiten en behoeften op een verschillende manier georganiseerd. Daarom wordt hier dus niet over de activiteiten gesproken, maar wel over de diensten, zelfs indien in sommige OCMW's de dienst slechts één enkele persoon telt of die ene persoon de activiteiten van verschillende diensten tegelijkertijd verricht.

Hieronder een aantal voorbeelden van diensten:

- dienst RMI,
- dienst schuldbemiddeling,
- dienst familiehulp,
- andere…

Die diensten hebben niet allemaal hetzelfde belang noch dezelfde dringendheid, maar streven wel dezelfde doelstellingen na: bijstand verlenen aan wie daarom vraagt.

Knowhow

6B. Knowhow

De knowhow van de maatschappelijk werkers, de administratieve ambtenaren en van het personeel in het algemeen speelt natuurlijk een essentiële rol: opdrachten behandelen, beheren en uitvoeren, maar ook problemen evalueren, zowel bij hun dagelijkse taken als bij de herneming van activiteiten en bij de inschatting van risico's.

Zo kan een bepaalde activiteit prioritair blijken. Veronderstellen we bijvoorbeeld dat de betaling van de leeflonen op vaste datum en uur topprioriteit

geniet. In dat geval zal het OCMW erop toezien dat de nodige aandacht wordt besteed aan de uitvoering van die activiteit, ongeacht zijn werkingsstatus. In geval van ramp kan de Raad voor Maatschappelijk Welzijn natuurlijk beslissen om één, twee of zelfs drie dagen of meer uit te trekken om opnieuw operationeel te worden en de leefloontrekkers uit te betalen.

De veiligheidsconsulent zal dus per dienst een inventaris van de activiteiten opmaken. Hij krijgt daarbij de hulp van de dienstverantwoordelijke, opdat geen enkel element over het hoofd wordt gezien dat noodzakelijk is voor de goede werking van de dienst.

Het diensthoofd en de veiligheidsconsulent schatten ook de risico's in, en doen gemeenschappelijke voorstellen om die in te perken.

Inventaris van de materiële behoeften

6C. Inventaris van de materiële behoeften.

Wat geldt voor de activiteiten van de diensten, geldt evenzeer voor de werkingsbehoeften.

Indien er zich ondanks het feit dat de risico's konden worden ingeperkt toch een ramp voordoet, moet de werking opnieuw kunnen worden opgestart. Door een inventaris op te stellen, kunnen sommige risico's trouwens beter gevat worden: staat van de elektrische installatie, staat van de muren en vloeren, barsten, blootstelling aan diefstal, onderhoud van de brandblusapparaten, enz.

Er wordt dus een inventaris opgesteld van het materieel dat de dienst(en) die opnieuw moet(en) opstarten nodig hebben, net als een inventaris van de informaticabehoeften.

Voorbeeld: hierna volgt de inventaris die betrekking heeft op de uitvoering van activiteit X:

- materiële inventaris: een stoel, een bureau, een telefoon, standaarddocumenten om aanvragen in te dienen bij de federale administratie, een fax, enz.
- inventaris van de informaticabehoeften: een klavier, een muis, een scherm, een pc, Windows XP met Word, Excel, programma XXX waarmee de schulden van mr. Y kunnen worden berekend, enz., een modem, een hub, 2 switches, een antivirusprogramma, een firewall, een back-up…

De maximaal aanvaardbare termijn bepalen

6D. De maximaal aanvaardbare termijn bepalen

Laten we aannemen dat de verantwoordelijke instantie (Raad voor Maatschappelijk Welzijn of het Bestendig Bureau) bepaald heeft dat de werking van een dienst voor een maximale duur van **X** dagen mag worden onderbroken.

Die maximale duur moet worden vastgesteld voor alle diensten van het OCMW die kaderen binnen de verwerking van sociale gegevens via de Kruispuntbank van de Sociale Zekerheid en binnen de prioritaire activiteiten.

Voorbeelden: dienst RMI: 72 u of 3 dagen,
dienst schuldbemiddeling: 120 u of 5 dagen,
dienst familiehulp: 96 u of 4 dagen.

Vervolgens worden de gemeenschappelijke punten van die uiteenlopende activiteiten in kaart gebracht en geanalyseerd. Op die manier kan worden voorzien in de middelen die een heropstart mogelijk maken en kan in een latere fase het rampenplan op basis van de aldus bepaalde prioriteiten worden opgesteld.

Voorbeeld: de Raad voor Maatschappelijk Welzijn heeft voor de heropstart van de dienst RMI, de dienst schuldbemiddeling en de dienst familiehulp een duur van vier dagen (96 u) toegekend.

Daarvoor zijn volgende zaken nodig:

- één of meer servers,
- de sociale software,
- back-ups,
- 5 bureaus voor 5 mensen,
- 3 telefoonlijnen,
- 5 antivirusprogramma's,
- 5 besturingssystemen,
- 1 Publilinkverbinding,
- een Dexia-betalingssysteem,
- 5 stoelen,
- 5 bureaus,
- 2 kasten,
- 1 fax
- enz.

Kan het OCMW zich al die elementen binnen de op grond van de risico's vooraf bepaalde termijn (4 dagen) aanschaffen?

Einde van de eerste stap.

Het OCMW beschikt nu over:

- een materiële inventaris,
- een inventaris van de informaticabehoeften,
- een maximale termijn die het in geval van ramp kan benutten om alle geïnventariseerde elementen aan te schaffen die noodzakelijk zijn voor de uitvoering van zijn activiteit(en).

In dit stadium kan het OCMW reeds het volgende vaststellen: wat dreigt er te ontbreken opdat de strategische activiteiten correct kunnen worden uitgevoerd? Die overweging geldt hier en nu. De risicoanalyse kan immers inderdaad een aantal gebreken (afwezigheid van nooddisks, inkt, airconditioning, enz.) of niet-materieelgerelateerde risico's (probleem met personeel, opleiding, informatie, wie herstelt of onderhoudt wat?) blootleggen.

Inventaris van de risico's

7. Inventaris van de risico's.

Na opmaak van de inventarissen worden de activiteiten van iedere dienst getoetst aan een aantal dreigingen, die hieronder worden opgesomd. Onderstaande lijst is niet exhaustief, want er zijn er ongeveer 250, maar iedere veiligheidsconsulent kan zelf bepalen wat hij voor zijn OCMW al dan niet als een dreiging beschouwt. Voorbeeld: vandalisme en brand. In de kolom naast de dreigingen vindt u de risico's die daaruit voortvloeien.

Dreigingen	Risico's
Stroomuitval.	Verlies van gegevens of van gegevensintegriteit (beschadiging van databanken, bijvoorbeeld, waardoor bepaalde gegevens niet langer juist zijn).
Al dan niet opzettelijke bewerkingsfout.	Verlies van gegevens, moeilijk om de juiste informatie te corrigeren of opnieuw in te voeren.
Virussen, wormen, trojaanse paarden, malware, spyware.	Verlies van informatie, van materieel (harde schijf), geen internettoegang meer, onomkeerbare bestandsvernietiging.
Misbruiken.	Verlies van vertrouwelijkheid en niet toegestane verspreiding van informatie indien onrechtmatige toegang tot vertrouwelijke informatie wordt verkregen.
Natuurrampen (buiten brand en aardbevingen), overstroming, storm, grondverzakking, andere.	Verlies van gegevens, van materieel, geen toegang meer tot informatie, onmogelijk de wettelijke taken van het OCMW uit te voeren.
Hacking (poging om het netwerk van binnenuit of van buitenaf binnen te dringen)	Verlies van vertrouwelijkheid, externe verspreiding van vertrouwelijke gegevens, eventuele verwijdering of wijziging van gegevens, toegangsblokkering, publicatie van gegevens op internet, enz.
Overbelasting van het informaticasysteem.	Slecht gebruik van het materieel (overbelasting van het geheugen, slechte synchronisatie van de omgevingen, gebrek aan updates, gebrek aan onderhoud) kan leiden tot werkings- en

	opslagproblemen die onomkeerbare gegevensverlies met zich meebrengen.
Falen back-upsysteem.	Verlies van gegevensopslag, onmogelijk opnieuw op te starten met een optimale basisconfiguratie, onmogelijk de oorsprong van de gegevens te controleren.
Brand.	Brand is een dreiging, maar de schade die veroorzaakt wordt door het bluswater is dat evenzeer. Er zijn velerlei risico's: onmogelijk om te beginnen werken, verlies van essentiële informatie, moeilijkheden om zich nieuw materieel of nieuwe software aan te schaffen, overeenkomstig financieel verlies (verplichting om de licenties opnieuw te kopen).

De secretaris, veiligheidsconsulent en informaticus (indien aanwezig) dienen vervolgens de lijst van de risico's per dienst te onderzoeken, net als de gevolgen die die zouden hebben voor de goede werking ervan. Hoe zouden die diensten opnieuw kunnen beginnen werken op basis van de geleden schade?

Het is aan te raden iedere dreiging per dienst te bekijken en de waarschijnlijkheid[2] in te schatten dat die dreiging zich effectief voordoet.

Voorbeeld.
Dienst uitbetaling RMI.
Plaats: lokaal 1ste verdieping.
Situatie: oud bureau, stalen meubels, grote concentratie van papier.
Inventaris: 2 pc's, 2 printers, 4 stoelen, 3 archiefkasten, 2 telefoontoestellen, 2 procedurehandboeken, …

Dreiging: diefstal.
Risico: laag, omdat er een inbraakdetectiesysteem is en het percentage diefstallen in de regio laag ligt. Bovendien heeft het publiek geen toegang tot de lokalen van de maatschappelijk assistenten.

[2] Waarschijnlijkheid dat die dreiging zich effectief voordoet: risico dat iets gebeurt, bijvoorbeeld: de waarschijnlijkheid van een auto-ongeval neemt toe met het jaarlijks aantal gereden kilometers. Iemand die 20 000 km/jaar rijdt, loopt een veel kleiner risico dan iemand die 100 000 km/jaar rijdt.

Dreiging: brand.

Risico: hoog. Het gebouw is oud en bevat veel hout. Niemand heeft een opleiding in brandbestrijding gevolgd en de brandweer bevindt zich op een afstand van 11 km. Geen enkele dienst zou het werk kunnen hervatten.

Uit de evaluatie van die dreigingen komen volgende elementen duidelijk naar voren:

- dankzij de identificatie van de dreigingen kan het OCMW die ondervangen of er een oplossing voor zoeken, om zo het risico of de risico's te beperken met het oog op de te verrichten strategische activiteiten;
- de analye van de dreigingen toont aan dat het OCMW kwetsbaar is indien het na een ramp zijn activiteiten moet hervatten.
- de noodzaak om een driejaarlijks veiligheidsplan uit te werken dat rekening houdt met de te ondervangen hiaten naargelang hun strategisch belang,
- de mogelijkheid voor het OCMW om zich voor te bereiden op incidenten waarvan de verschillende ernstigheidsgraad niet altijd dezelfde investeringen maar wel dezelfde aanpak vereist.

Prioritair of niet?

8. Prioritair of niet ?

Op basis van de specifieke situatie van het OCMW, op basis van zijn geografische ligging, op basis van het personeel (bijvoorbeeld: de informatie zit bij een enkele persoon) maakt de veiligheidsconsulent een inventaris op van de dreigingen en de risico's, bekijkt hij die samen met de verantwoordelijke van het dagelijks beheer en stelt hij acties voor om het risico of de risico's in te perken. Hij doet er goed aan om een of meerdere prioriteiten op te geven, die na goedkeuring door de Raad voor Maatschappelijk Welzijn in de min of meer

nabije toekomst zullen worden aangepakt. De andere acties ter inperking van de risico's worden in zijn driejaarlijks plan opgenomen.

Einde van de tweede stap.

Het OCMW beschikt nu over een inventaris van de dreigingen en de risico's. De veiligheidsconsulent heeft vastgesteld of die al dan niet prioritair moeten worden ingeperkt. Indien er prioriteiten zijn, neemt hij die op in zijn planning of in zijn driejaarlijks veiligheidsplan.

Actie

9. Resultaten - Actie.

Deze risicoanalyse heeft betrekking op:

- enerzijds, de sociale gegevens die door het OCMW en via de Kruispuntbank van de Sociale Zekerheid worden beheerd;
- anderzijds de behoeften waaraan moet worden voldaan om een betrouwbaar rampenplan uit te werken.

Deze analyse reikt een aantal belangrijke en nuttige adviezen aan die het OCMW moeten toelaten zijn zwakke punten aan te pakken en te verbeteren. Zoals elders geldt ook hier dat voorkomen beter is dan genezen. Het is dus zaak de nodige voorbereidingen te treffen en te weten hoe problemen kunnen worden rechtgezet.

Op basis van die analyse moeten er acties worden genomen om het risico of de risico's in te perken, waarbij diverse prioriteitscriteria gehanteerd worden:

- het belang van het risico,
- het belang van de dienst voor het OCMW,
- het belang van de aan te wenden middelen.

Onderstaande tabel wil de veiligheidsconsulent helpen de hierboven uiteengezette logica te volgen en het proces te vergemakkelijken.
Vergeet nooit dat het risicobeheer altijd moet worden besproken met en gedragen door de verantwoordelijke van het dagelijks beheer.

G. Kempgens
Veiligheidsconsulent POD MI

Voorbeeldtabel om het begrip van de risicoanalyse te vergemakkelijken.

Dienst	Dreigingen	Gevolgen	Risico-niveau[3]	Rechtvaardi-ging	Noodzakelijke actie om het risico in te perken	Vervangbaar / niet vervangbaar binnen de vooropgestelde termijnen	Uitgevoerd – niet uitgevoerd	Prioritair – niet prioritair
Dienst: RMI. **Heropstart voor de dienst RMI: 3 werkdagen**								
Leefloon	Stroom-onderbreking	Gegevensverlies in het informatica-systeem	L	Er zijn heel weinig stroompannes. Bovendien beschikt het informatica-systeem over een UPS (batterij) waardoor gegevens-verlies kan worden vermeden.	Over een UPS beschikken	Snelle vervanging.	In orde	NR[4]
		Kwetsbaar worden van het informatica-materieel.	L	De UPS fungeert als stabilisator voor de stroom-voorziening.	Idem	Idem	In orde	NR

[3] L = laag, dus geen actie nodig, G = gemiddeld, dus reageren naargelang het risico, H = hoog, snel reageren om het risico weg te werken.

[4] NR = niet relevant omdat alles in orde is.

Dienst	Dreigingen	Gevolgen	Risico-niveau[5]	Rechtvaardi-ging	Noodzakelijke actie om het risico in te perken	Vervangbaar / niet vervangbaar binnen de vooropgestelde termijnen	Uitgevoerd – niet uitgevoerd	Prioritair – niet prioritair
Leefloon	Overstroming	Vernietiging van gegevens. Vernietiging van het informatica-materieel. Vernietiging van archieven. Vernietiging van informaticadragers (back-up).	G	De informatica-dienst bevindt zich onder een Velux. In geval van lek zal het water tot in de stopcontacten sijpelen die zich in de vloer bevinden.	Een waterdetector installeren die gekoppeld is aan de brandcentrale. Smeltzekering installeren. De archieven ofwel elders ofwel op hoger gelegen schappen plaatsen. De gegevensback-ups zullen gered worden, maar de back-ups van de boekhouding niet.	Ja omdat de back-ups extern worden opgeslagen. Ja omdat de leverancier zich ertoe verbonden heeft het materieel snel te vervangen. Nee omdat de archieven op de grond staan en niet vervangen kunnen worden. Alle back-ups extern opslaan.	Ja. Ja, maar informeel engagement. Nee. Nee.	Nee. Gemiddel-de prioriteit. Ja. Ja.

[5] L = laag, dus geen actie nodig, G = gemiddeld, dus reageren naargelang het risico, H = hoog, snel reageren om het risico weg te werken.

Dienst	Dreigingen	Gevolgen	Risico-niveau[6]	Motieven en gevolgen	Noodzakelijke actie om het risico in te perken	Vervangbaar / niet vervangbaar binnen de vooropgestelde termijnen	Uitgevoerd – niet uitgevoerd	Prioritair – niet prioritair
Leefloon	Update antivirus-programma	Vernietiging van gegevens. Eventuele vernietiging van harde schijven. Geen internettoegang. Mogelijkheid tot intrusie. Mogelijkheid tot gegevensdiefstal.	H	Probleem van recurrente updates. De updates functioneren niet naar behoren en het antivirus-programma wordt soms gedurende een week niet geüpdatet.	Contact opnemen met de leverancier en zorgen dat er functionele updates worden verkregen.	Nee. Verplichting om nieuw materieel te kopen en heel de serverconfiguratie en de gegevens opnieuw te installeren.	Nee.	Prioritair.

[6] L = laag, dus geen actie nodig, G = gemiddeld, dus reageren naargelang het risico, H = hoog, snel reageren om het risico weg te werken.

Blanco tabel voor de veiligheidsconsulenten.

Dienst	Dreigingen	Gevolgen	Risico-niveau[7]	Motieven en gevolgen	Noodzakelijke actie om het risico in te perken	Vervangbaar / niet vervangbaar binnen de vooropgestelde termijnen	Uitgevoerd – niet uitgevoerd	Prioritair – niet prioritair
Dienst: **Heropstarttermijn:**								

[7] L = laag, dus geen actie nodig, G = gemiddeld, dus reageren naargelang het risico, H = hoog, snel reageren om het risico weg te werken.