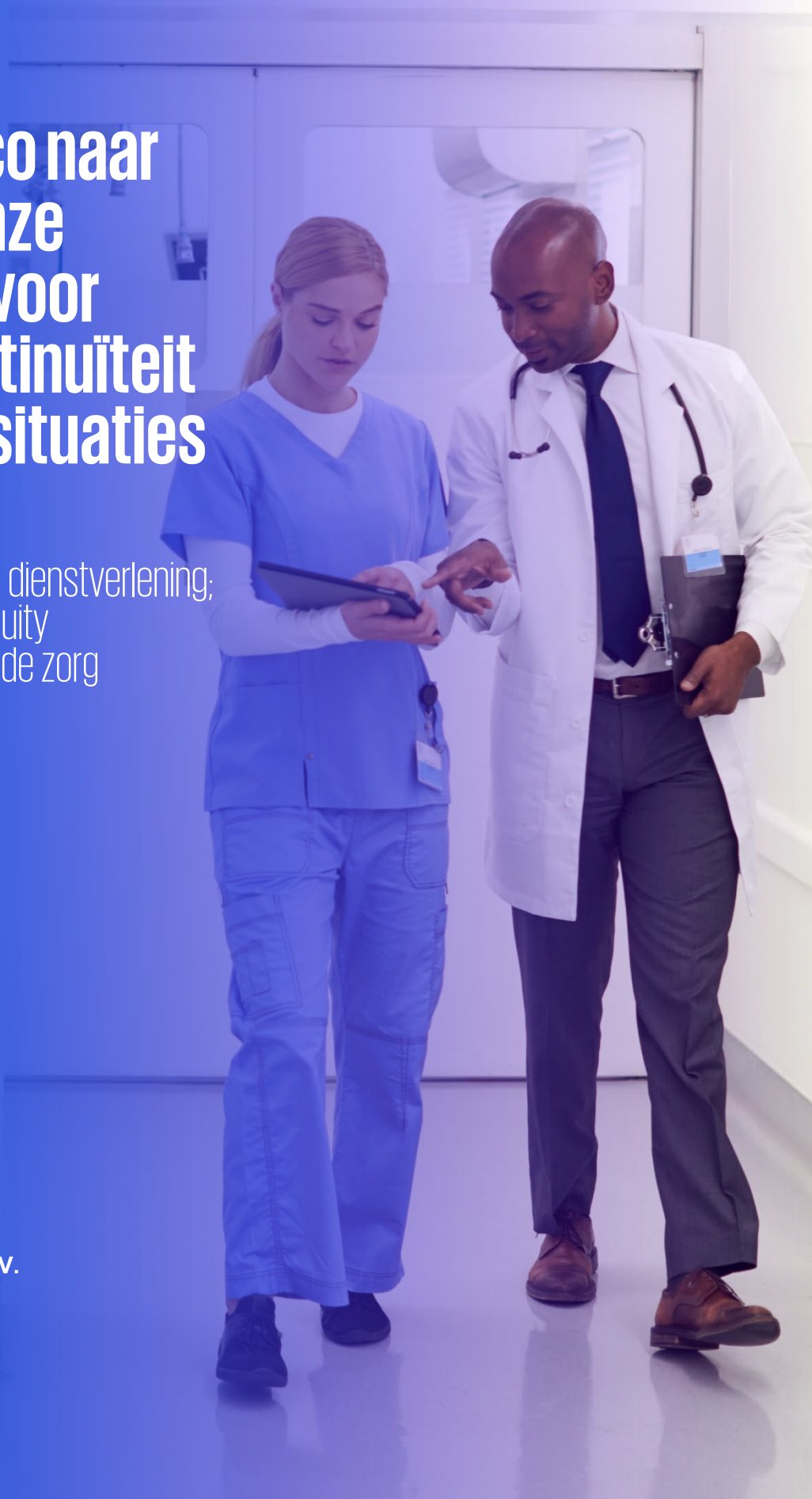
Van risico naar regie: onze aanpak voor zorgcontinuïteit in crisissituaties

Onze aanpak en dienstverlening; Business Continuity Management in de zorg



KPMG Advisory N.V.

—

Juni 2025

Zorgcontinuïteit in een veranderende wereld: voorbereid op grootschalige verstoringen

Realiteit: risico's die zorg overstijgen

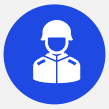
De wereld verandert snel en brengt nieuwe risico's met zich mee voor de zorgsector. Door geopolitieke spanningen, klimaatverandering en digitale afhankelijkheid neemt de kans op grootschalige verstoringen, zoals wateroverlast, stroomuitval of cyber-aanvallen, toe. De situatie in Oekraïne en signalen van sabotage maken duidelijk dat zulke scenario's ook Nederland kunnen raken. In zulke omstandigheden is verhoogde inzet van zorgpersoneel cruciaal, terwijl tegelijkertijd de beschikbaarheid onder druk kan staan doordat medewerkers zelf geraakt worden – emotioneel, praktisch of familiair. Dit vraagt om een zorgsector die voorbereid is, snel kan opschalen en effectief samenwerkt.

Toch zijn veel protocollen voor rampenopvang (ZiROP), crisiscommunicatie en paraatheid nog niet aangescherpt of geoefend. De urgentie om nu te handelen is groot.

Business Continuity Management (BCM) speelt hierin een sleutelrol. Het helpt zorgorganisaties niet alleen hun eigen continuïteit te waarborgen, maar ook bij te dragen aan de weerbaarheid van de hele zorgketen. Dit document beschrijft onze visie en aanpak: hoe wij zorginstellingen ondersteunen bij het versterken van veerkracht, het organiseren van regionale samenwerking en het vertalen van risico's naar regie.

Casuïstiek: Wat als het misgaat?

Oorlogsdreiging en Oekraïne



Door toenemende internationale spanningen en de reële kans op directe betrokkenheid van Nederland bij een conflict, dreigt een plotselinge, grootschalige instroom van patiënten. Tegelijkertijd kan zorgpersoneel zelf geraakt worden – emotioneel, praktisch of familiair – waardoor de beschikbare zorgcapaciteit nog meer onder druk komt te staan.

Overstromingen in Wallonië, Duitsland en Zuid-Limburg

Deze overstromingen in 2021 leidden tot grootschalige evacuaties van zorginstellingen. Hoewel het water langzaam kwam, bleek de voorbereiding vaak onvoldoende. De logistiek van evacuatie, communicatie met ketenpartners en het waarborgen van continuïteit bleken grote uitdagingen.

Grootschalige cyberaanval in Groot-Brittannië

De Britse gezondheidsdienst NHS werd in 2017 getroffen door de wereldwijde WannaCry-ransomwareaanval. Ziekenhuizen verloren toegang tot patiëntgegevens, operaties werden uitgesteld en spoeddiensten omgeleid. Deze aanval toonde aan hoe kwetsbaar ziekenhuizen en zorginstellingen kunnen zijn zonder basismaatregelen voor digitale weerbaarheid.

Stroomuitval in Spanje en Portugal

In april 2025 vond een grootschalige stroomstoring plaats in Spanje en Portugal. Ziekenhuizen en zorgorganisaties moesten overschakelen op noodplannen, zonder te weten hoe lang de situatie zou duren. Organisaties konden niet rekenen op acute hulp van de (landelijke) overheid aangezien de hele regio getroffen werd.

Verstoringen in leveringen als gevolg van handelsoorlog

De fabriek van Philips in Best (Nederland), die onder andere MRI- en röntgenscanners produceert, levert wereldwijd aan ziekenhuizen. Door de handelsoorlog moeten ze de productie verplaatsen en hun toeleveringsketen aanpassen. Dit leidt mogelijk tot vertragingen in leveringen van apparatuur aan ziekenhuizen.

Wereldwijde pandemie

COVID-19 ontregelde de normale gang van zaken wereldwijd. Lockdowns en de avondklok konden overbelasting van de zorgsector niet voorkomen. Het werd snel duidelijk dat de maatschappij niet opgewassen was tegen deze enorme druk op de toeleveringsketen en een gebrek aan actie-intelligentie zorgden voor capaciteits- en personeelsdruk van ongekende mate.

Eén aanpak, vele oplossingen: gericht op wat nu nog geen prioriteit krijgt

Crisisoorzaken en de noodzaak voor effectieve respons

Op basis van eerdere crisissen hebben we inzicht verkregen in de stressfactoren die een significante invloed kunnen hebben op de continuïteit van zorg. Wij onderscheiden drie soorten stressfactoren die de noodzaak voor respons creëren.

1. Wereldwijde externe stressfactoren

Internationale ontwikkelingen zoals geopolitieke spanningen, klimaatverandering en cyberdreigingen kunnen onverwacht en ingrijpend doorwerken in de zorg. De Wet weerbaarheid kritieke entiteiten (Wwke) – de Nederlandse invulling van de EU Critical Entities Resilience Directive – verplicht zorgorganisaties om hun weerbaarheid aantoonbaar te versterken. Samen met de aankomende Cyberbeveiligingswet benadrukt deze regelgeving dat risico's vaak grensoverschrijdend zijn.

2. Regionale externe stressfactoren

Regionale rampen, zoals extreme weerscenario's of stroomstoringen, zijn vaak plotseling, tastbaar en lastig te beheersen. Ze raken meerdere zorginstellingen tegelijk en leggen de kwetsbaarheid van lokale infrastructuur bloot. Daarom is het cruciaal te investeren in robuuste infrastructuur én regionale samenwerking. Dit sluit aan bij de Whole of Society-aanpak van KPMG, waarin publieke en private partijen gezamenlijk werken aan regionale veerkracht, gedeelde capaciteiten en voorbereidheid op crisissituaties.

3. Interne stressfactoren

Interne stressfactoren, zoals uitval, tekorten of verstoringen in menselijke of geautomatiseerde processen, kunnen minstens zo ontwrichtend zijn voor de continuïteit van zorg. Juist daarom is een sterke interne basis essentieel. Dit vraagt om heldere protocollen, goed getraind personeel en een organisatie die snel kan schakelen. Het ontwikkelen van actie-intelligentie – het vermogen om onder druk doelgericht te handelen – maakt het verschil tussen impactvolle verstoring en effectieve crisisrespons.

Primaire focus van Business Continuity Management (regio-overstijgend)

Primaire focus van zorginstellingen, ziekenhuizen en regionale samenwerkingsverbanden

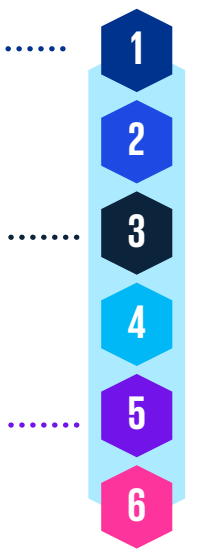
Onze aanpak op hoofdlijnen

Voor de uitvoering van onze dienstverlening hanteren we een standaardaanpak op hoofdlijnen als leidraad. De aanpak bestaat uit **zes fasen**. Deze aanpak is het resultaat van onze ervaring en expertise met betrekking tot vergelijkbare casussen. Hierbij komen kennis, cyber- en risicomanagement samen in één model.

Scope van het BCM-programma vastleggen
- Ecosysteem in kaart brengen, stakeholders identificeren en inzicht krijgen in logistieke afhankelijkheden.

Opstellen van strategie met het oog op continuïteit
- Strategieën ontwikkelen met het oog op continuïteit en risicomanagement.
- Potentiële alternatieve werkwijzen instellen voor essentiële zorgactiviteiten.

Medewerkers voorzien van doelgerichte training
- Medewerkers voorzien van opleidingen, training en oefeningen om hen optimaal voor te bereiden op potentiële crisissen, bijvoorbeeld door middel van een tapletop-oefening of andere scenario-based simulaties.
- Evalueren van continuïteitsplannen door systeemtesten uit te voeren met de medewerkers.



Potentiële risico's en valkuilen identificeren
- Specifieke (potentiële) pijnpunten identificeren in het omgaan met risico's.
- Impact en belang van verschillende risico's bestuderen.
- Prioriteren van sleutelrisico's op basis van hun impact en de waarschijnlijkheid van voorkomen.
- Beoordelen van de bestaande beheersmaatregelen.

Opstellen van plannen met het oog op continuïteit
- Opstellen van plannen die continuïteit moeten waarborgen.
- Uitvoeren van een scenarioanalyse om mogelijke reacties op bestaande risico's in kaart te brengen.
- Het intern beschikbaar stellen van plannen voor alle medewerkers en teams.

Continuïteitsplannen monitoren en onderhouden
- Werking voortdurend controleren op effectiviteit en efficiëntie.
- Aanpassingen doorvoeren bij wijzigende situatie of risico's.
- Plan aanpassen aan nieuwe wetten of veranderende noden in de zorg.

Onze aanpak om de zorgsector te ondersteunen met het opbouwen van een weerbaar systeem

Onze aanpak in detail

Iedere organisatie is uniek en vraagt om een aanpak om weerbaarheid te borgen en goed voorbereid te zijn op disruptieve evenementen. Afhankelijk van de behoeften en situatie van de organisatie en opdrachtgever past KPMG zijn aanpak aan en stemt deze af op de specifieke context.

KPMG werkt vanuit een Whole of Society-aanpak, waarbij weerbaarheid wordt gezien als een gedeelde verantwoordelijkheid van zorginstellingen, overheid, leveranciers en burgers. Door deze brede blik helpt KPMG organisaties niet alleen met technische oplossingen, maar ook met governance, bewustwording en samenwerking. In het artikel 'Cyberweerbaarheid versterken: een noodzakelijke stap voor ziekenhuizen' stellen wij dat een nationale aanpak noodzakelijk is voor digitale weerbaarheid in de zorg. Niet elke instelling kan zelfstandig alle risico's afdekken. Door samenwerking, kennisdeling en gezamenlijke investeringen kan de sector als geheel robuuster worden — een cruciale voorwaarde voor continuïteit in tijden van crisis.

KPMG heeft uitgebreide ervaring in het begeleiden van zorginstellingen bij het versterken van hun weerbaarheid tegen verstoringen – zowel op digitaal als fysiek gebied. Deze casussen illustreren hoe kwetsbaarheden in de praktijk zichtbaar worden en hoe gerichte interventies bijdragen aan structurele verbetering van de continuïteit van zorg.

De casus 'Van 'onbewust kwetsbaar' naar betere cyberveiligheid' biedt concrete handvatten voor zorginstellingen om cybersecurity te integreren in bredere BCM-strategieën. Denk aan governance, risicomanagement, scenario-oefeningen en het versterken van de menselijke factor. De rode draad: continuïteit begint bij bewustzijn en eindigt bij structurele borging. Een krachtig instrument dat KPMG hierbij inzet is Red Teaming: realistische simulaties van cyberaanvallen om kwetsbaarheden in systemen, processen en gedrag bloot te leggen. Zo werd bij een topklinisch ziekenhuis een aanval gesimuleerd waarbij het Red Team ongezien toegang kreeg tot kritieke systemen zoals het EPD. Deze oefening leidde tot concrete verbetermaatregelen, waaronder versnelde cloudmigratie en versterkte monitoring.

Crisismanagement in een complex tijdperk

In een tijd waarin verstoringen in de zorg steeds ingrijpender en complexer worden – van oorlogen en pandemieën tot cyberdreigingen en personeelstekorten – is een doordachte aanpak van Business Continuity Management essentieel. De continuïteit van zorgverlening staat onder druk en het beheersen van risico's vraagt om meer dan alleen reactief handelen. Het vereist een integrale, toekomstgerichte benadering, die aansluit bij de dynamiek van de zorgsector.

Een effectief BCM-programma biedt structuur, inzicht en handelingsperspectief. Het maakt risico's beheersbaar, vergroot de veerkracht van de organisatie en ondersteunt bij het maken van verantwoorde keuzes – ook onder druk. Transparantie en herleidbaarheid zijn daarbij cruciaal, net als het vermogen om snel te schakelen bij veranderende omstandigheden.
Bestuurders en toezichthouders hebben in deze context steeds vaker behoefte aan een onafhankelijke partner die niet alleen risico's scherp analyseert, maar ook helpt bij het implementeren van sterke maatregelen die passend zijn voor de doelstellingen en strategie van de organisatie.

KPMG biedt deze objectieve blik en combineert diepgaande kennis van de zorg met expertise in risico- en crisismanagement. Zo helpen wij zorginstellingen om voorbereid te zijn op het onverwachte – en om de zorg voor morgen veilig te stellen.

Hokkie Blogg
Partner, Business Continuity & Crisis Management
M: +31 6 5335 5232
E: blogg.hokkie@kpmg.nl

Arjan Ogink
Partner, Strategy & Operations Healthcare
M: +31 6 4826 3503
E: ogink.arjan@kpmg.nl

Michiel Beijersbergen
Senior Manager, Business Continuity & Crisis Management
M: +31 6 1334 5669
E: beijersbergen.michiel@kpmg.nl

Dennis Utermark
Director, Cyber
M: +31 6 3047 7661
E: utermark.dennis@kpmg.nl

Henrik Smit
Director, Defense & Response
M: +31 6 1255 6514
E: smit.henrik@kpmg.nl

Max Roelofs
Consultant, Business Continuity & Crisis Management
M: +31 6 104 534410
E: roelofs.max@kpmg.nl

Appendix – KPMG hanteert bewezen raamwerken en modellen voor heldere inzichten en adviezen

KPMG's visie op Business Resilience

Business Resilience is het vermogen om de levering van kritieke producten en diensten in stand te houden en, indien mogelijk, uit te breiden tijdens en na significante verstoringen. Business Continuity Management is een preventieve activiteit die bijdraagt aan deze veerkracht en weerbaarheid, door belangrijke rollen en verantwoordelijkheden te definiëren en continuïteitsstrategieën op te stellen. Hierbij zijn risico-identificatie en -evaluatie, voorbereiding op verstoringen, weerbaarheid versterken, vertrouwen van stakeholders en conformiteit met wetten en regels cruciaal.

KPMG's tijdlijn voor crisis management

Het vermogen van een organisatie om niet alleen incidenten en crisissen te detecteren als ze zich voordoen, maar er ook effectief op te reageren en ervan te herstellen, wordt steeds kritischer bekeken. Het crisismanagementraamwerk (CMF) van een organisatie vormt de basis voor escalatie, communicatie en coördinatie tijdens een crisis. Het biedt ook de structuur voor het trainen en oefenen van belanghebbenden met verantwoordelijkheden op het gebied van crisismanagement.

Links naar KPMG-publicaties