

Weerbaarheidchecklist

Een praktisch BCM-instrument voor Ondernemers

Wat is BCM?

Business Continuity Management (BCM) zorgt ervoor dat jouw bedrijf ook bij verstoringen blijft functioneren. Denk aan stroomuitval, cyberaanval of het uitvallen van een sleutelpersoon. Deze checklist helpt je de basis op orde te krijgen, ook als je er nog nooit mee bezig bent geweest. Nutsuitval (stroom, water, gas, internet) is apart uitgelicht omdat dit de meest voorkomende en direct merkbare verstoringen zijn.

Deze checklist is onderdeel van de Handreiking Ondernemend in crisistijd. De checklist is tot stand gekomen in samenwerking met vertegenwoordiging van gemeenten, het bedrijfsleven, veiligheidsregio's en diverse partners die in directe verbinding staan met ondernemers.

Hoe gebruik je dit?

Doorloop alle secties en vink aan wat geregeld is. Gebruik de kolom 'Opmerking / Actie' voor vervolgstappen. Noteer alles wat nog ontbreekt in het actieplan achteraan. Streef niet naar perfectie. Elke stap die je zet verkleint je risico.

ALGEMEEN	Bedrijf:	
	Datum:	
	Ingevuld door:	
	Functie:	
	Bedrijfslocatie:	



DEEL A NUTSVOORZIENINGEN - Stroom, Water, Gas & Internet

Print deze tabel uit en plak hem in de meterkast, serverruimte en bij de balie.			
NOODCONTACTEN	Netbeheerder / Stroomleverancier	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
	Waterbedrijf	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
	Gasleverancier / Netbeheer	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
	Internetprovider (zakelijk)	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
	IT-beheerder / Helpdesk	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
	Verhuurder / Gebouwbeheerder	Storingsnummer	
		Klantnummer	
		Max. uitvalduur	
		Noodmaatregel	
Verzekeraar (schade melden)	Storingsnummer		
	Klantnummer		
	Max. uitvalduur		
	Noodmaatregel		



Let op: Sla de storingspagina van jouw netbeheerder op als bladwijzer op je telefoon: www.enexis.nl/storingen-en-onderhoud. Die werkt ook als je vaste internet eruit ligt.

STROOMUITVAL	Actiepunt	Status	Opmerking/Actie
	Ik weet welke processen direct uitvallen bij stroomstoring - servers, kassa, koeling, productie, verlichting	Ja Nee	
	Er is een Uninterruptible Power Supply (UPS) aanwezig voor servers, netwerk en kassasystemen - beschermt bij korte uitval en spanningspieken	Ja Nee	
	Kritieke apparatuur heeft een aggregaat of huurcontract voor noodstroomvoorziening - bijv. koelcellen, productielijn, zorgapparatuur	Ja Nee	
	Het aggregaat wordt minimaal 1x per kwartaal getest onder belasting - en de brandstofvoorraad wordt regelmatig gecontroleerd	Ja Nee	
	Gevoelige apparatuur is beveiligd tegen spanningspieken bij het terugkeren van stroom	Ja Nee	
	Laptops en mobiele apparaten zijn altijd (deels) opgeladen - zodat medewerkers minimaal een halve werkdag mobiel kunnen werken	Ja Nee	
	Medewerkers weten wat ze moeten doen bij stroomuitval - schriftelijke procedure aanwezig en bekend	Ja Nee	
	Noodverlichting en vluchtrouteaanduidingen zijn op accu en jaarlijks getest	Ja Nee	



Tip: De meeste stroomstoringen duren minder dan 4 uur. Een UPS (€150–400) is voor kantooromgevingen al voldoende om ordelijk af te sluiten. Test het aggregaat echt — niet alleen aanzetten, maar ook onder volledige belasting.

WATERUITVAL	Actiepunt	Status	Opmerking/Actie
	Ik weet welke processen afhankelijk zijn van stromend water - productie, koeling, sanitair, brandblussing	Ja Nee	
	Er is een noodvoorraad drinkwater aanwezig - minimaal 1,5 liter per persoon per dag voor 48 uur	Ja Nee	
	Bij uitval van warm water is er een noodprocedure - bijv. koelcellen, productielijn, zorgapparatuur	Ja Nee	
	Koelingsinstallaties die op water draaien hebben een uitwijkoptie of temperatuuralarm	Ja Nee	
	De locatie van de hoofdkraan is bekend bij alle medewerkers en direct bereikbaar	Ja Nee	



Tip: Wateruitval is voor kantoren meestal snel oplosbaar. Voor productie- en zorginstellingen is dit een kritisch scenario — breng afhankelijkheden expliciet in kaart, ook richting je verzekeraar.

GASUITVAL	Actiepunt	Status	Opmerking/Actie
	Ik heb een overzicht van alle processen die gas gebruiken - verwarming, keuken, productie, drogers, stoomketels	Ja Nee	
	Er is een alternatieve verwarmingsbron voor de winterperiode - elektrische kachels, infrarood, tijdelijke warmteunit	Ja Nee	
	Bij gasuitval in de productie is er een uitwijkprocedure of wordt de klant direct geïnformeerd	Ja Nee	
	Alle medewerkers weten hoe ze de hoofdgaskraan afsluiten	Ja Nee	
	Horeca / kantine: er is een alternatief voor voedselbereiding bij gasuitval	Ja Nee	



Tip: Gasuitval is zeldzamer maar treft harder in de winter. Zorg dat je minimaal 48 uur zonder gasverwarming kunt functioneren met beschikbare alternatieven.



Let op: Ruik je gas? Gaskraan direct sluiten, pand verlaten, 112 bellen.
Gebruik géén elektrische apparaten of lichtschakelaars — dit kan een vonk veroorzaken.

INTERNET & TELECOMSTORING	Actiepunt	Status	Opmerking/Actie
	Er is een back-up internetverbinding via 4G/5G-router of tweede provider - meest effectieve maatregel — meteen inzetbaar	Ja Nee	
	Medewerkers kunnen via mobiele hotspot tijdelijk doorwerken bij kabelstoring	Ja Nee	
	Cloudapplicaties zijn offline of via 4G bereikbaar - Microsoft 365 offline, Google Drive gesynchroniseerd, lokale kopieën	Ja Nee	
	VoIP-telefonie heeft een noodomleiding naar mobiel bij internetuitval	Ja Nee	
	Klanten en leveranciers kennen een mobiel nummer als e-mail of website uitvalt	Ja Nee	
	De hersteltijdgarantie (SLA) van je internetprovider is bekend en vastgelegd	Ja Nee	
	Kritieke data staat ook lokaal opgeslagen — niet uitsluitend in de cloud	Ja Nee	



Tip: Een 4G/5G-zakenrouter als noodlijn (€30–80/mnd) is voor de meeste bedrijven de beste investering. Internetstoring is veruit de meest voorkomende zakelijke calamiteit — en ook het makkelijkst op te vangen.

DEEL B BEDRIJFSCONTINUÏTEIT - Plan, Mensen, Data & Financiën

KEN JE RISICO'S	Actiepunt	Status	Opmerking/Actie
	Ik heb een lijst van mijn 5 grootste risico's - nutsuitval, cyberaanval, brand, ziekte sleutelpersoon, leverancier valt weg	Ja Nee	
	Ik weet welke processen het meest kritiek zijn - zonder welke activiteit valt mijn omzet direct weg?	Ja Nee	
	Ik weet hoe lang mijn bedrijf maximaal kan stilliggen (RTO) - bijv. max. 4 uur of max. 1 dag per kritiek proces	Ja Nee	
	Ik weet hoeveel dataverlies ik me kan veroorloven (RPO) - bijv. max. 24 uur aan transacties kwijt zijn	Ja Nee	
	Ik heb de afhankelijkheden van kritieke leveranciers en partners in kaart	Ja Nee	
	Ik heb nagedacht over gecombineerde uitval - bijv. stroom én internet tegelijk bij storm	Ja Nee	



Tip: Begin simpel: schrijf op één A4 je 3 grootste angstscenario's en wat er dan stopt. Dat is al 80% van een bruikbare risicoanalyse. Verfijn daarna.

NOODPLAN & CRISISMANAGEMENT	Actiepunt	Status	Opmerking/Actie
	Er is een noodplan — ook al is het maar 1 A4 - minimaal: scenario, wie beslist, wie communiceert, hoe klanten bereiken	Ja Nee	
	Er is een crisiscoördinator aangewezen - één persoon die in een calamiteit beslissingen neemt	Ja Nee	
	Het noodplan is bekend bij minimaal 2 andere personen in het bedrijf	Ja Nee	
	Er is een belijst met wie ik bij welk scenario als eerste bel - thuiswerken, coworking, locatie van partner of klant	Ja Nee	
	Er is een uitwijklocatie als het pand onbruikbaar is - klanten, leveranciers, verzekeraar, IT-partner, netbeheerder	Ja Nee	
	Het noodplan is ook offline beschikbaar (geprint) - werkt ook zonder stroom en internet	Ja Nee	
	Het noodplan wordt minimaal 1x per jaar besproken of getest met het team	Ja Nee	



Tip: Een noodplan hoeft geen dik boekwerk te zijn. Één pagina met: wat is er mis, wie doet wat, hoe bereiken we klanten - dat is al genoeg om gestructureerd te handelen tijdens stress.

DATA & IT-BEVEILIGING	Actiepunt	Status	Opmerking/Actie
	Alle kritieke bedrijfsdata wordt minimaal dagelijks automatisch geback-up't	Ja Nee	
	Back-ups staan op een andere locatie of in de cloud - 3-2-1 regel: 3 kopieën, 2 media, 1 offsite of cloud	Ja Nee	
	Ik heb de back-up het afgelopen jaar minimaal 1x teruggeplaatst (restore-test) - niet alleen maken, ook daadwerkelijk terugzetten	Ja Nee	
	Alle medewerkers gebruiken sterke wachtwoorden én tweefactorauthenticatie (2FA)	Ja Nee	
	Werkcomputers worden automatisch bijgewerkt met beveiligingsupdates	Ja Nee	
	Er is antivirussoftware actief op alle werkplekken	Ja Nee	
	Er is een procedure als een medewerker op een phishinglink heeft geklikt - wie bel je, wat doe je direct?	Ja Nee	
	Toegangsrechten worden beheerd - ex-medewerkers worden direct geblokkeerd	Ja Nee	



Tip: De 3-2-1-back-upregel: 3 kopieën van je data, op 2 verschillende opslagmedia, waarvan 1 offsite of in de cloud. Testen of je de back-up kunt terugzetten is minstens zo belangrijk als het maken ervan.

SLEUTELPERSONEN & KENNISBORING	Actiepunt	Status	Opmerking/Actie
	Kritieke taken en werkprocessen zijn gedocumenteerd zodat een ander het kan overnemen	Ja Nee	
	Voor elke kritieke functie is een vervanger of achternvanger benoemd	Ja Nee	
	Inloggegevens en toegangscode zijn veilig opgeslagen én bereikbaar voor een achternvanger - bijv. wachtwoordmanager of beveiligde kluis	Ja Nee	
	Er zijn afspraken bij langdurige ziekte - via collega-ondernemer, uitzendbureau of ZZP-kracht	Ja Nee	
	Er zijn volmachten voor bankrekeningen en contracten bij ziekte of overlijden van de eigenaar	Ja Nee	



Tip: Maak een 'hit-by-a-bus'-document: één pagina per sleutelpersoon met de belangrijkste wachtwoorden, contacten en lopende taken. Bewaar dit in een kluis of via een notaris.

LEVERANCIERS & KETENRISICO	Actiepunt	Status	Opmerking/Actie
	Mijn kritieke leveranciers zijn geïdentificeerd - zonder wie staat mijn bedrijf direct stil?	Ja Nee	
	Van elke kritieke leverancier ken ik een alternatief of een uitwijkoptie	Ja Nee	
	Contracten met kritieke leveranciers bevatten afspraken over continuïteit en hersteltijd	Ja Nee	
	Ik ben niet volledig afhankelijk van één leverancier voor een kritiek product of dienst	Ja Nee	
	Bij uitval van een kritieke leverancier is er een noodinkoop- of uitwijkprocedure	Ja Nee	



Tip: Vraag je drie meest kritieke leveranciers of zij zelf een continuïteitsplan hebben. Het geeft je inzicht én dwingt hen na te denken over hun eigen weerbaarheid.

VERZEKERINGEN & FINANCIËN	Actiepunt	Status	Opmerking/Actie
	Mijn bedrijfsverzekeringen zijn actueel en afgestemd op mijn huidige risico's	Ja Nee	
	Ik heb een bedrijfsschadeverzekering (omzetdervingsverzekering) afgesloten	Ja Nee	
	Ik weet wat mijn verzekeraar vergoedt bij nutsuitval, brand, overstrooming en cyberaanval	Ja Nee	
	Er is een financiële buffer voor minimaal 3 maanden vaste lasten	Ja Nee	
	Ik heb een kredietlijn of noodlening achter de hand als inkomsten wegvallen	Ja Nee	
	Ik weet bij welke instanties (RVO, UWV, gemeente) ik terecht kan bij een calamiteit	Ja Nee	



Tip: Bespreek jaarlijks je polis met een onafhankelijk verzekeringsadviseur. Veel ondernemers zijn onderverzekerd — zeker bij cyberschade en bedrijfsonderbreking door nutsuitval.

COMMUNICATIE	Actiepunt	Status	Opmerking/Actie
	Ik heb een actuele contactenlijst van klanten en leveranciers ook offline beschikbaar	Ja Nee	
	Er is een kant-en-klaar sjabloon voor een eerste communicatiebericht bij een storing	Ja Nee	
	Klanten weten via welk kanaal ze mij bereiken als e-mail en website uitvallen - mobiel nummer, WhatsApp, LinkedIn	Ja Nee	
	Er is een aangewezen woordvoerder bij een crisis - wie mag namens het bedrijf naar buiten communiceren?	Ja Nee	
	Medewerkers weten wat ze wel en niet mogen communiceren bij een incident	Ja Nee	



Tip: Een korte, eerlijke mededeling ('We ondervinden een verstoring en verwachten herstel binnen X uur') is altijd beter dan stilte. Communiceer proactief — ook als je nog geen oplossing hebt.

Jouw BCM-score

Tel alle aangevinkte punten op

Punten	Advies	Wat nu?
43 - 54 punten	Goed op weg! Zorg dat je noodplan ook getest is en jaarlijks wordt bijgehouden.	Onderhoud & jaarlijks testen
27 - 42 punten	Basis aanwezig, maar er zijn nog belangrijke gaten. Focus op de onbeantwoorde punten.	Vul de gaten - gebruik het actieplan
0 - 26 punten	Direct actie nodig. Begin vandaag met noodcontacten, back-ups en een noodplan van 1 A4.	Start met: noodplan + IT + noodcontacten

Noteer hier de 5 acties die je na het invullen van deze checklist direct oppakt. Wees concreet: wat, wie en wanneer af?

MIJN ACTIEPLAN	Actie	Deadline	Wie?
	1		
	2		
	3		
	4		
	5		