GIDS

Business continuity planning & advies

BIA, BCP, disaster recovery, ISO 22301, NIS2-compliance en kosten. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De meeste Nederlandse bedrijven hebben geen business continuity plan. De cijfers laten zien waarom dat een risico is.

80%
van het MKB heeft geen business continuity plan -- het laagste maturiteitsniveau in Europa
Siemens / Graydon / KVK [1]

40%
van bedrijven gaat failliet binnen 1 jaar na een calamiteit zonder BCP
Interpolis [2]

EUR 115K
gemiddelde kosten per storing voor Nederlandse bedrijven
ARP Solutions [3]

3×/maand
gemiddeld aantal verstoringen per bedrijf -- van IT-uitval tot stroomstoring
ARP Solutions [3]

75%
van bedrijven zonder BCP gaat failliet binnen 3 jaar na ernstige IT-problemen
Invenioit / diverse bronnen [4]

Q2 2026
verwachte inwerkingtreding Cyberbeveiligingswet -- BCP wettelijk verplicht voor 17 sectoren
Rijksoverheid [5]

50--70%
sneller herstel na een incident voor organisaties met een actueel BCP
Highberg [6]

EUR 10M
maximale boete bij NIS2 non-compliance -- of 2% van de wereldwijde jaaromzet
NCSC / NIS2-richtlijn [7]

1. Wat is business continuity planning?

Business continuity planning (BCP) is het proces waarmee je je organisatie voorbereidt op langdurige verstoringen. Het doel: kritieke bedrijfsprocessen laten doordraaien, ongeacht wat er gebeurt.[1]

Een BCP gaat verder dan een IT-noodplan. Het dekt alle kritieke processen -- van facturering en logistiek tot klantcommunicatie en personeelsbezetting. Of de verstoring nu een cyberaanval is, een brand, een pandemie of een leveranciersuitval: je hebt vooraf nagedacht over hoe je doorgaat.[8]

BCP VS DRP VS ITSCM -- WAT IS HET VERSCHIL?

TERM	TYPE	SCOPE	WAT KRIJG JE?
BCP	Preventief document	Alle kritieke processen	Herstelstrategieen, noodprocedures, communicatieplan
BCM	Managementsysteem	Organisatiebreed	BCP + governance, training, oefeningen, continue verbetering
BIA	Analyse-instrument	Kritieke processen	Impact-assessment, RTO/RPO, prioritering
DR	Technisch plan	IT-systemen	Backup, restore, failover, IT-herstel
Crisismanagement	Reactief proces	Incident-specifiek	Crisisorganisatie, communicatie, besluitvorming
ISO 22301	Certificeringsnorm	BCM-systeem	Internationale standaard voor bedrijfscontinuiteitsmanagement

> **Kernverschil:** BCP is het plan zelf. BCM is het bredere managementsysteem waarin dat plan leeft. Disaster recovery is specifiek IT-gericht, terwijl BCP alle bedrijfsprocessen dekt. De BIA is de analytische basis waarop het BCP wordt gebouwd.[8][9]

WAAROM HET MEER IS DAN ALLEEN IT

Veel organisaties verwarren BCP met een disaster recovery plan. Maar een BCP gaat over de hele organisatie:[10]

- **Personeel** -- Wie neemt taken over als medewerkers uitvallen? Is er een opvolgingsplan?
- **Locatie** -- Kun je elders werken als je kantoor onbereikbaar is?

- **Leveranciers** -- Heb je alternatieven als je belangrijkste toeleverancier wegvalt?
- **Communicatie** -- Wie communiceert naar klanten, media en medewerkers bij een crisis?
- **IT-systemen** -- Disaster recovery is een onderdeel van BCP, niet het geheel

2. Waarom is het belangrijk?

De cijfers zijn helder: bedrijven zonder BCP overleven calamiteiten zelden. De kosten van niet-voorbereid zijn overtreffen de investering in een BCP met grote marge.

DE HARDE CIJFERS

STATISTIEK	DETAIL	BRON
40% failliet	Binnen 1 jaar na een calamiteit zonder BCP	Interpolis[2]
60%+ failliet	Binnen 2 jaar na een calamiteit	Interpolis[2]
75% failliet	Binnen 3 jaar na ernstige IT-problemen (zonder BCP)	Diverse bronnen[4]
50% MKB failliet na brand	De helft van MKB-bedrijven overleeft een brand niet	Rabobank / IFV[11]
3 verstoringen/maand	Gemiddeld aantal verstoringen per bedrijf	ARP Solutions[3]
EUR 115.000 per storing	Gemiddelde kosten per verstoring in Nederland	ARP Solutions[3]

KOSTEN VAN DOWNTIME PER SECTOR

SECTOR	KOSTEN PER UUR DOWNTIME
E-commerce (piekperiode)	USD 1--2 miljoen
Automotive	USD 2,3 miljoen
Manufacturing	USD 500.000 -- 1 miljoen
Ziekenhuizen	USD 318.000 -- 540.000
Gemiddeld alle sectoren	USD 336.000 (benchmark)

Bron: Oxford Economics / Erwood Group [12][13]

BELANGRIJK

80% van het MKB heeft geen BCP.[1] De voornaamste reden: men weet niet hoe te beginnen, of onderschat het risico. Met de NIS2-wetgeving op komst wordt dit een wettelijk probleem bovenop een bedrijfsrisico.

ROI VAN BUSINESS CONTINUITY

Voorbeeld ROI-berekening (MKB):

Investering BCP-traject: EUR 15.000 (eenmalig) + EUR 3.000 jaarlijks onderhoud.
Gemiddelde kosten 1 dag downtime: EUR 50.000+.
Break-even: na 1 voorkomen verstoring van meer dan 3 uur.[6]

3. Hoe werkt het?

Een BCP-traject volgt een gestructureerd pad: van analyse naar plan, van plan naar oefening, en van oefening naar onderhoud. Hieronder de stappen.

1 Business Impact Analyse (BIA)

2--6 WEKEN

Het fundament. Je identificeert alle kritieke processen, kwantificeert de impact van uitval, en stelt per proces een Recovery Time Objective (RTO) en Recovery Point Objective (RPO) vast. Zonder BIA bouw je op aannames.[9][14]

2 Risicoanalyse

2--4 WEKEN

Welke dreigingen zijn realistisch voor jouw organisatie? Cyberaanval, brand, stroomuitval, personeelsuitval, leveranciersfalen? Per dreiging beoordeel je waarschijnlijkheid en impact.[8]

3 BCP-strategie bepalen

1--2 WEKEN

Per kritiek proces bepaal je de herstelstrategie: uitwijklocatie, thuiswerken, handmatige fallback, alternatieve leverancier, of accepteren van tijdelijke uitval.

4 BCP-document schrijven

2--4 WEKEN

Het daadwerkelijke plan: noodprocedures per scenario, communicatieprotocollen, verantwoordelijkheden, contactlijsten, en herstelstappen. Pragmatisch en bruikbaar -- geen boekwerk dat niemand leest.[10]

5 Disaster Recovery Plan

2--4 WEKEN

Het IT-specifieke onderdeel: backup-strategie, failover-procedures, herstelprocedures per systeem, en een testschema. Dit is een deelplan binnen het grotere BCP.[3]

6 Crisismanagementplan

1--2 WEKEN

Wie beslist wat tijdens een crisis? Escalatieprocedures, woordvoering, interne en externe communicatie. Dit plan zorgt dat je in de eerste uren niet verlamd raakt.

7 Testen en oefenen

DOORLOPEND

Een plan dat niet getest is, werkt niet. Minimaal jaarlijks een tabletop exercise (scenario doorlopen met het team) en een technische DR-test (daadwerkelijk herstellen vanuit backup).[15]

8 Onderhoud en review

DOORLOPEND

Na elke wijziging in je organisatie, IT-landschap of leverancierssketen: plan bijwerken. Minimaal jaarlijks een volledige review en management sign-off.[10]

TOTALE DOORLOOPTIJD

TRAJECT	DOORLOOPTIJD	TOELICHTING
Basis-BCP (MKB)	2--3 maanden	Met template, beperkte scope, 1 locatie
Volledig BCP (middelgroot)	3--6 maanden	BIA + BCP + DR-plan, meerdere afdelingen
BCM-systeem (enterprise)	6--15 maanden	Volledig BCM incl. governance, training, oefenprogramma
ISO 22301 certificering	9--18 maanden	Van nul naar gecertificeerd BCM-systeem

4. Wat kost het?

De kosten van een BCP-traject hangen af van je organisatiegrootte, complexiteit en ambitieniveau. Hieronder de bandbreedte voor de Nederlandse markt.

BCP-ADVIESTRAJECTEN

SEGMENT	INDICATIE KOSTEN	WAT ZIT ERIN
MKB (< 50 medewerkers)	EUR 5.000 -- 15.000	BIA (beperkt), BCP-document, DR-basisplan, 1 tabletop exercise
Middelgroot (50--250)	EUR 15.000 -- 40.000	Volledige BIA, BCP, DR-plan, crisismanagementplan, 2--3 oefeningen
Enterprise (250+)	EUR 40.000 -- 100.000+	Uitgebreide BIA alle locaties, volledig BCM-systeem, meerdere DR-plannen, jaarlijks oefenprogramma

UURTARIEVEN SPECIALISTEN

ROL	UURTARIEF (INDICATIE)	TOELICHTING
BCM-consultant (ZZP)	EUR 100 -- 150	BIA, BCP opstellen, implementatie
Senior BCM-adviseur (bureau)	EUR 150 -- 225	Strategie, complexe trajecten, ISO 22301
Crisismanagement-specialist	EUR 150 -- 250	Crisisorganisatie, oefeningen, coaching
IT DR-specialist	EUR 110 -- 175	Disaster recovery, backup-architectuur

Het gemiddelde uurtarief van een freelance consultant in Nederland ligt in 2025 op EUR 120 excl. btw.[16][17]

ISO 22301 CERTIFICERING

KOSTENCOMPONENT	INDICATIE	TOELICHTING
Implementatie-begeleiding	EUR 10.000 -- 30.000	Afhankelijk van organisatiegrootte en huidige maturiteit
Initiele certificeringsaudit	EUR 5.000 -- 15.000	Stage 1 + Stage 2 audit door geaccrediteerde instelling

KOSTENCOMPONENT	INDICATIE	TOELICHTING
Jaarlijkse controle-audit	EUR 3.000 -- 8.000	50--70% van initiele auditkosten
Her-certificering (3-jaarlijks)	EUR 4.000 -- 12.000	Volledige heraudit

TIP

Totale kosten eerste jaar ISO 22301 (MKB): EUR 15.000 -- 45.000 (implementatie + certificering). Doorlopend: EUR 3.000 -- 8.000 per jaar voor controle-audits plus interne capaciteit.[18][19]

5. Waar moet je op letten?

Een BCP-traject staat of valt met de juiste partner. Hieronder de criteria waarmee je aanbieders kunt vergelijken -- zonder namen, maar met concrete toetsstenen.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
ISO 22301 kennis	Certificeringservaring garandeert dat het plan aan internationale standaarden voldoet
Sectorervaring	Een adviseur die jouw sector kent, begrijpt de specifieke risico's en compliance-eisen
Praktische aanpak	Een bruikbaar plan van 20 pagina's is waardevoller dan een boekwerk van 200 pagina's
BIA-methodiek	Vraag hoe ze de Business Impact Analyse uitvoeren -- dit is het fundament van elk goed BCP
Integratie met IT	BCP en DR moeten op elkaar aansluiten -- de adviseur moet IT-kennis hebben of samenwerken met je IT-partner
Oefenprogramma	Een plan zonder test is een plan op papier. Kies een partij die ook oefeningen en simulaties biedt
Onderhoud en nazorg	Een BCP veroudert snel. Vraag naar een onderhoudscontract of jaarlijkse review
NIS2-kennis	Met de Cyberbeveiligingswet op komst moet je BCP aan wettelijke eisen voldoen

10 VRAGEN AAN JE BCP-ADVISEUR

STEL DEZE VRAGEN VOOR JE TEKENT

1. Hoe voer je de Business Impact Analyse uit? Welke methodiek gebruik je?
2. Hoeveel BCP-trajecten heb je in mijn sector begeleid?
3. Wat is de gemiddelde doorlooptijd voor een organisatie van mijn omvang?
4. Hoe zorg je dat het plan bruikbaar blijft en niet in een la verdwijnt?
5. Welke oefenvormen bied je aan? (tabletop, simulatie, technische DR-test)
6. Hoe integreer je het BCP met ons bestaande disaster recovery plan?
7. Voldoet het eindresultaat aan NIS2/Cyberbeveiligingswet-eisen?
8. Bied je ondersteuning bij ISO 22301 certificering?
9. Wat is inbegrepen in de prijs en wat zijn meerkosten?
10. Kun je referenties delen van vergelijkbare trajecten?

TIP

Vraag altijd naar een concreet voorbeeld van een BCP dat de adviseur eerder heeft opgeleverd. Je ziet dan direct of het plan pragmatisch en bruikbaar is, of een theoretisch document.

6. Veelgemaakte fouten

De meeste BCP-trajecten mislukken niet door een gebrek aan budget, maar door verkeerde aannames en onvoldoende aandacht na de oplevering.

#	FOUT	GEVOLG	HOE VOORKOMEN
1	Alleen IT-focus (DR = BCP)	Niet-IT processen vergeten: personeel, leveranciers, locatie	BCP = alle kritieke processen. DR is slechts een onderdeel[10]
2	Plan op de plank	Plan is verouderd en onbruikbaar als het nodig is	Minimaal jaarlijks updaten, na elke organisatiewijziging reviewen[15]
3	Niet testen	Fouten komen pas aan het licht tijdens een echte crisis	Minimaal jaarlijks een tabletop exercise + technische DR-test[15]
4	Geen management-commitment	Budget en capaciteit ontbreken, plan verwatert	Bestuurders verantwoordelijk maken -- NIS2 verplicht dit ook[5]
5	Te complex	Niemand leest het plan, onbruikbaar in een crisissituatie	Focus op de top-10 scenario's, pragmatisch houden
6	Geen BIA uitgevoerd	Plan gebaseerd op aannames, verkeerde prioriteiten	Altijd starten met een BIA: kwantificeer impact per proces[9]
7	Uitbesteden zonder interne betrokkenheid	Plan sluit niet aan bij de werkelijkheid	Dwarsdoorsnede van organisatie betrekken (MT, HR, IT, operations)
8	Communicatieplan ontbreekt	Chaos in communicatie naar medewerkers, klanten en media	Communicatieprotocollen vooraf vastleggen, inclusief woordvoering
9	Afhankelijkheden niet in kaart	Uitval leverancier legt eigen processen plat	Supply chain dependencies meenemen in de BIA[14]
10	Risico's accepteren zonder bewuste keuze	Pandemie of supply chain-verstoring als verrassing	Elk geaccepteerd risico expliciet documenteren met onderbouwing

MEEST VOORKOMEND

De combinatie van fouten 1, 2 en 3 -- alleen IT-focus, plan op de plank, nooit getest -- komt het vaakst voor bij MKB-bedrijven. Het resultaat is een plan dat er op papier goed uitziet, maar in de praktijk waardeloos is.[10]

7. Compliance: NIS2 en de Cyberbeveiligingswet

De NIS2-richtlijn maakt business continuity planning wettelijk verplicht voor duizenden Nederlandse organisaties. Artikel 21 noemt bedrijfscontinuiteit expliciet als verplichte maatregel.

WAT NIS2 EIST

De NIS2-richtlijn (EU 2022/2555) wordt in Nederland geimplementeerd via de Cyberbeveiligingswet (Cbw), die naar verwachting in Q2 2026 van kracht gaat. Artikel 21 lid 1 sub c eist:[5][7]

> "bedrijfscontinuiteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheersing"

VEREISTE	WAT HET INHOUDT
Bedrijfscontinuiteitsplan	Scenario's en herstelstrategieen voor kritieke diensten
Backup-management	Backupstrategie: frequentie, opslag, testschema
Herstelplannen	Recovery procedures om na een incident terug te keren naar normale operatie
Crisismanagement	Crisisorganisatie, escalatieprocedures, communicatieprotocollen
Testen	Regelmatige oefeningen en tests van continuiteitsplannen

WIE VALT ERONDER?

NIS2 onderscheidt 17 sectoren verdeeld over essentiele en belangrijke entiteiten:[20]

Essentiele entiteiten (proactief toezicht): energie, transport, bankwezen, financiele markten, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, ICT-dienstverlening, overheid, ruimtevaart.

Belangrijke entiteiten (reactief toezicht): postdiensten, afvalbeheer, chemische industrie, voedselproductie, productie medische hulpmiddelen, digitale dienstverleners, onderzoeksinstellingen.

Grootterecriteria: In principe bedrijven met meer dan 50 medewerkers of meer dan EUR 10 miljoen omzet. Sommige sectoren (DNS, TLD-registries) vallen er ongeacht grootte onder.

SANCTIES BIJ NON-COMPLIANCE

TYPE	SANCTIE
Boete essentiele entiteiten	Tot EUR 10 miljoen of 2% van wereldwijde jaaromzet
Boete belangrijke entiteiten	Tot EUR 7 miljoen of 1,4% van wereldwijde jaaromzet
Bestuurdersaansprakelijkheid	Persoonlijke aansprakelijkheid van bestuurders, mogelijke schorsing
Reputatieschade	Openbare bekendmaking van non-compliance

ISO 22301 ALS FRAMEWORK VOOR NIS2

ISO 22301 certificering is niet verplicht voor NIS2-compliance, maar dient als een sterk framework om aan de BCP-vereisten te voldoen. Er is circa 70% overlap tussen ISO 22301 en de NIS2 BCP-vereisten.[18][21]

TIP

Begin niet met ISO 22301 certificering als doel op zich. Gebruik het als framework voor je BCP, en beslis later of formele certificering meerwaarde biedt voor tenders of klantrelaties.

8. Verschil: BCP vs DRP vs incident response vs cyberverzekering

Business continuity, disaster recovery, incident response en cyberverzekeringen worden vaak door elkaar gehaald. Ze vullen elkaar aan, maar dekken verschillende risico's op verschillende momenten.

ASPECT	BCP	DRP	INCIDENT RESPONSE	CYBERVERZEKERING
Focus	Alle kritieke bedrijfsprocessen	IT-systemen en data	Beveiliging: detectie en reactie op incidenten	Financiele schade na een incident
Wanneer	Preventief + tijdens crisis	Na IT-uitval	Tijdens en direct na een beveiligingsincident	Na een incident (schadeafwikkeling)
Scope	Organisatiebreed	IT-infrastructuur	Cybersecurity-incidenten	Financieel (schade, aansprakelijkheid)
Output	Continuiteitsplan met herstelstrategieen	Technische herstelprocedures	Playbooks, forensisch onderzoek	Polis met dekking en premie
Wie	Management + alle afdelingen	IT-afdeling	Security team / SOC	Verzekeraar
NIS2	Verplicht (art. 21)	Verplicht (onderdeel BCP)	Verplicht (art. 21)	Niet verplicht, wel aanbevolen

> **Hoe ze samenwerken:** Incident response detecteert en beperkt de aanval. Het DRP herstelt de IT-systemen. Het BCP zorgt dat de organisatie kan doordraaien terwijl dat gebeurt. De cyberverzekering dekt de financiele schade die overblijft.[8][3]

PRAKTIJKVOORBEELD

Een ransomware-aanval raakt je bedrijf:

1. **Incident Response** -- SOC detecteert de aanval, isoleert getroffen systemen, start forensisch onderzoek
2. **DRP** -- IT herstelt systemen vanuit backups, schakelt over naar secundaire omgeving
3. **BCP** -- Crisisteam activeert noodprocedures, klanten worden geinformeerd, kritieke processen draaien handmatig of via alternatieve kanalen
4. **Cyberverzekering** -- Dekt kosten van forensisch onderzoek, omzetverlies, herstelkosten en eventuele aansprakelijkheid

9. Trends 2025--2026

Business continuity verandert van een IT-aangelegenheid naar een strategisch bedrijfsproces. Deze trends bepalen de richting.

CYBER RESILIENCE

De focus verschuift van "herstellen na een incident" naar "doordraaien tijdens een incident". Cyber resilience combineert BCP, incident response en disaster recovery tot een geintegreerde aanpak. Organisaties investeren in het vermogen om aanvallen te absorberen zonder dat de bedrijfsvoering stopt.[22]

INTEGRATED RISK MANAGEMENT

BCP wordt steeds vaker onderdeel van een breder risk management framework. In plaats van geisoleerde plannen per domein (IT, compliance, operationeel) kiezen organisaties voor een geintegreerde aanpak waarin risico's over domeinen heen worden beoordeeld.[6]

BCP-AS-A-SERVICE

Voor MKB-bedrijven die geen interne BCM-capaciteit hebben, ontstaan managed BCP-diensten. Een externe partij beheert je BCP, voert periodieke reviews uit, organiseert oefeningen en houdt het plan actueel. Vergelijkbaar met hoe managed security services (SOC-as-a-Service) de markt hebben veranderd.

AI-GESTUURDE SCENARIO PLANNING

AI-tools worden ingezet om scenario's te modelleren en de impact van verstoringen te simuleren. Dit maakt het mogelijk om sneller en frequenter te testen zonder de operationele belasting van traditionele oefeningen. De technologie staat nog aan het begin, maar de eerste toepassingen zijn er.[22]

HYBRIDE DREIGINGEN

Crises in 2026 zijn steeds vaker hybride incidenten met cascading effecten:[22]

- Cyberaanval leidt tot reputatieschade leidt tot operationele uitval
- Personeelstekort veroorzaakt kwaliteitsproblemen veroorzaakt leveringsproblemen
- Geopolitieke spanning verstoort supply chains, drijft prijzen op, vergroot klantdruk

> **Drie drivers voor marktgroei:**
>
> 1. **NIS2/Cyberbeveiligingswet** -- wettelijke verplichting voor 17 sectoren.
> 2. **Supply chain eisen** -- klanten vereisen BCP van leveranciers in tenders.
> 3. **Verzekeringsmarkt** -- premiekortingen bij aantoonbaar BCM-beleid.[6][22]

10. Aan de slag

Je weet nu wat BCP inhoudt, wat het kost, en waarom het belangrijk is. Tijd om te handelen.

DE EERSTE STAPPEN

1 Breng je kritieke processen in kaart

Welke processen moeten absoluut doordraaien? Wat gebeurt er als ze 1 uur, 1 dag of 1 week uitvallen? Dit is de kern van een BIA en het startpunt van elk BCP.

2 Bepaal je risicoprofiel

Welke dreigingen zijn realistisch voor jouw organisatie? Cyberaanval, brand, stroomuitval, personeelsuitval? Prioriteer op waarschijnlijkheid en impact.

3 Check je NIS2-status

Val je onder de Cyberbeveiligingswet? Met meer dan 50 medewerkers of meer dan EUR 10 miljoen omzet in een van de 17 sectoren is de kans groot. In dat geval is BCP wettelijk verplicht.

4 Zoek de juiste partner

Gebruik de selectiecriteria uit hoofdstuk 5 en de 10 vragen om aanbieders te vergelijken. Kies een partij met sectorervaring, een pragmatische aanpak en een oefenprogramma.

HULP NODIG BIJ HET KIEZEN?

Op **ibgids.nl/word-gematcht** vul je in wat je zoekt en matchen wij je met gekwalificeerde BCP-adviseurs die passen bij jouw sector, organisatiegrootte en budget. Onafhankelijk en kosteloos.

WAT JE VANDAAG AL KUNT DOEN

- **Maak een lijst** van je 5 meest kritieke bedrijfsprocessen
- **Stel de vraag** aan je MT: wat doen we als [proces X] morgen uitvalt?
- **Check je backups** -- wanneer zijn ze voor het laatst getest?
- **Controleer je verzekering** -- dekt je polis bedrijfsschade door IT-uitval?
- **Plan een gesprek** met een BCP-adviseur via ibgids.nl/word-gematcht

AAN DE SLAG

Ga naar **ibgids.nl/word-gematcht** en ontvang binnen 48 uur voorstellen van BCP-specialisten die bij jouw situatie passen.

Bronnenlijst

Alle bronnen die in deze gids worden aangehaald, met directe links.

[1] **KVK** -- Bedrijfscontinuiteitsplan: blijf overeind na een ramp.
https://www.kvk.nl/veilig-zakendoen/goed-voorbereid-op-een-calamiteit/

[2] **Crisismanagement Academie** -- Bedrijfscontinuiteitsplan Opstellen in 2026.
https://crisismanagement-academie.nl/bedrijfscontinuiteitsplan-opstellen/

[3] **ARP Solutions** -- Minder downtime met een disaster recovery plan.
https://www.arpsolutions.nl/kennisbank-trends/it-blogs/minder-downtime-met-een-disaster-recovery-plan

[4] **Invenioit** -- 25 Business Continuity Statistics to Know.
https://invenioit.com/continuity/business-continuity-statistics/

[5] **Rijksoverheid** -- Implementatie NIS2 en CER in Nederland.
https://www.rijksoverheid.nl/actueel/nieuws/2024/10/23/implementatie-nis2-en-cer-in-nederland-vertraagd-wat-betekent-dat-voor-u

[6] **Highberg** -- De ROI van business continuity management.
https://highberg.com/nl/insights/de-roi-van-business-continuity-management-de-kosten-op-de-juiste-plek

[7] **NCSC** -- Zorgplicht NIS2.
https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn

[8] **KPN Zakelijk** -- Een business continuity plan opstellen in zeven stappen.
https://www.kpn.com/zakelijk/thedigitaldutch/blog/business-continuity-plan-in-zeven-stappen

[9] **ICTRecht** -- Hoe voer je een Business Impact Analyse uit?
https://www.ictrecht.nl/blog/hoe-voer-je-een-business-impact-analyse-uit

[10] **Digital Trust Center (Min. van EZ)** -- Hoe maak je een Bedrijfscontinuiteitsplan?
https://www.digitaltrustcenter.nl/nis2/hoe-maak-je-een-bedrijfscontinuiteitsplan

[11] **Kader Group** -- Plan bedrijfscontinuiteit MKB: wat, waarom en hoe.
https://kader.nl/actueel/plan-bedrijfscontinu%C3%AFteit-mkb-wat,-waarom-en-hoe/

[12] **Erwood Group** -- The True Costs of Downtime in 2025.
https://www.erwoodgroup.com/blog/the-true-costs-of-downtime-in-2025-a-deep-dive-by-business-size-and-industry/

[13] **Oxford Economics / Cockroach Labs** -- The State of Resilience 2025.
https://www.cockroachlabs.com/blog/the-state-of-resilience-2025-reveals-the-true-cost-of-downtime/

[14] **ICTRecht** -- Business Impact Analyse voor informatiebeveiliging.
https://www.ictrecht.nl/blog/waarom-is-een-business-impact-analyse-essentieel-voor-uw-informatiebeveiliging

[15] **Grant Thornton** -- De zin en onzin van een Business Continuity Plan.
https://www.grantthornton.be/insights/articles/de-zin-en-onzin-van-een-business-continuity-plan/

[16] **Knab** -- ZZP-uurtarieven 2025: alle relevante cijfers.
https://bieb.knab.nl/ondernemen/zzp-uurtarieven-2025-alle-relevante-cijfers-per-sector-beroep-en-specialisatie

[17] **Consultancy.nl** -- Consultancy Tarieven.
https://www.consultancy.nl/adviesbranche/consultancy-tarieven

[18] **TUV NORD** -- Wat is ISO 22301 certificering?
https://www.tuv.nl/nl/diensten-en-certificeringen/iso-certificeringen/iso-22301-certificering/

[19] **CertificeringsAdvies Nederland** -- ISO 22301 certificering.
https://certificeringsadvies.nl/kwaliteit/iso-22301/

[20] **NCTV** -- Welke organisaties vallen onder de Cyberbeveiligingswet?
https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/welke-organisaties-vallen-onder-de-cyberbeveiligingswet

[21] **IB&P** -- Bedrijfscontinuiteit volgens BIO, NIS2, ISO 27001 en NEN 7510.
https://ib-p.nl/2024/06/bedrijfscontinuiteit-volgens-bio-nis2-iso-27001-en-nen-7510/

[22] **Risk and Resilience Hub** -- 23 Business Continuity Statistics You Need to Know.
https://riskandresiliencehub.com/23-business-continuity-statistics-you-need-to-know/

[23] **OfficeGrip** -- Het belang van bedrijfscontinuiteit volgens NIS2.
https://officegrip.nl/het-belang-van-beveiligingsaspecten-van-bedrijfscontinuiteit-volgens-nis2/

[24] **Financieel Management** -- Maak een Business Continuity Plan in 6 stappen.
https://financieel-management.nl/artikel/maak-een-business-continuity-plan-in-6-stappen/

[25] **SURF** -- Starterkit Business Continuity Management (PDF).
https://www.surf.nl/files/2019-03/Starterkit_Business_Continuity_Management.pdf