FSMA
AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN

Circulaire

FSMA_2016_03 dd. 1/03/2016

Gezonde beheerpraktijken inzake de bedrijfscontinuïteit van gereglementeerde ondernemingen

Toepassingsveld:

Deze circulaire is van toepassing op :
- de vennootschappen voor vermogensbeheer en beleggingsadvies naar Belgische recht;
- de beheervennootschappen van (alternatieve) instellingen voor collectieve belegging naar Belgisch recht;
- de Belgische bijkantoren van vennootschappen voor vermogensbeheer en beleggingsadvies en van beheervennootschappen van (alternatieve) instellingen voor collectieve belegging, die ressorteren onder het recht van een staat die geen lid is van de Europese Unie.

Samenvatting/Doelstelling:

Deze circulaire somt, in de vorm van gezonde beheerpraktijken, een aantal criteria op aan de hand waarvan de FSMA het bedrijfscontinuïteitsbeleid van de gereglementeerde ondernemingen onder haar toezicht zal toetsen.

Structuur:

1. Verantwoording en definities
2. Toepassingsgebied
3. Vastlegging van een bedrijfscontinuïteitsbeleid door de onderneming
4. Invulling van het bedrijfscontinuïteitsbeleid
5. Betrokkenheid van externe dienstverleners

Bijlage 1 - Criteria voor de bepaling van de minimumafstand tussen de ICT-centra en de -uitwijkcentra

1. Verantwoording en definities

De vennootschappen voor vermogensbeheer en beleggingsadvies en de beheervennootschappen van (alternatieve) instellingen voor collectieve belegging moeten over een voor hun activiteiten passende organisatie beschikken[1].

Deze vergunningsvereiste houdt onder meer in dat de betrokken ondernemingen alle redelijke middelen inzetten om hun dienstverlening en activiteiten zonder onderbrekingen te verzekeren. Rekening houdend met de aard, de omvang en de complexiteit van hun activiteiten, dienen zij hun organisatie, hun systemen en hun procedures meer bepaald zo op te zetten dat zij de verplichtingen die uit hun toezichtstatuut voortvloeien, bij een ernstige en niet-geplande onderbreking van hun activiteiten, kunnen blijven nakomen en de belangen en de rechten van hun cliënten kunnen vrijwaren.

In het licht daarvan is een aangepast bedrijfscontinuïteitsbeleid een noodzakelijk instrument om die doelstellingen te kunnen verwezenlijken.

Deze circulaire somt, in de vorm van gezonde beheerpraktijken, een aantal criteria op aan de hand waarvan de FSMA het bedrijfscontinuïteitsbeleid van de gereglementeerde ondernemingen onder haar toezicht zal toetsen.

Deze circulaire vervangt met onmiddellijke ingang de circulaire PPB 2005/2 in verband met gezonde beheerpraktijken inzake de bedrijfscontinuïteit van financiële instellingen.

---

[1] Zie artikel 62 van de wet van 6 april 1995 inzake het statuut van en het toezicht op de beleggingsondernemingen, artikel 221 van de wet van 3 augustus 2012 betreffende de instellingen voor collectieve belegging die voldoen aan de voorwaarden van Richtlijn 2009/65/EG en de instellingen voor belegging in schuldvorderingen, artikel 4, § 3 van het Koninklijk besluit van 12 november 2012 met betrekking tot de beheervennootschappen van instelling voor collectieve belegging, artikel 33 van de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders en artikel 57, § 3 van de gedelegeerde verordening nr. 231/2013 van de Commissie van 12 december 2012 tot aanvulling van Richtlijn 2011/61/EU van het Europees Parlement en de Raad ten aanzien van vrijstellingen, algemene voorwaarden voor de bedrijfsuitoefening, bewaarders, hefboomfinanciering, transparantie en toezicht.

In deze circulaire wordt verstaan onder:

bedrijfscontinuïteit:	de doelstelling om de dienstverlening en de activiteiten in alle omstandigheden ongestoord te laten verlopen;
bedrijfscontinuïteitsbeleid:	het vastleggen van een bedrijfscontinuïteitsstrategie en een uitvoeringsbeleid dat erop is gericht om alle redelijke maatregelen te nemen om de bedrijfscontinuïteit te verzekeren;
bedrijfscontinuïteitsplanning:	het plannings- en voorbereidingsproces dat, ter uitvoering van het bedrijfscontinuïteitsbeleid, in een bedrijfscontinuïteitsplan uitmondt;
bedrijfscontinuïteitsplan, verkort "BCP":	een verzameling van procedures en documentatie die wordt ontwikkeld en tot een coherent geheel wordt gebundeld, en vervolgens ter beschikking wordt gehouden voor het geval zich een niet-geplande onderbreking voordoet.

2. Toepassingsgebied

2.1. *Ratione personae*

De gezonde beheerpraktijken zijn van toepassing op de vennootschappen voor vermogensbeheer en beleggingsadvies en de beheervennootschappen van (alternatieve) instellingen voor collectieve belegging naar Belgisch recht. Zij zijn ook van toepassing op de Belgische bijkantoren van vennootschappen voor vermogensbeheer en beleggingsadvies en van beheervennootschappen van (alternatieve) instellingen voor collectieve belegging die ressorteren onder het recht van een staat die geen lid is van de Europese Unie.

Voor ondernemingen die deel uitmaken van een groep, kan de groepsdimensie een belangrijke rol spelen bij de definitie en de tenuitvoerlegging van hun bedrijfscontinuïteitsbeleid. De onderneming moet in dat geval aantonen dat de organisatie op groepsniveau geen afbreuk doet aan de deugdelijkheid van haar bedrijfscontinuïteitsbeleid.

De gezonde beheerpraktijken zijn relevant voor zowel grote als kleine ondernemingen, hoewel de gevolgen van onderbrekingen voor elk bedrijf erg verschillend kunnen zijn. Daarom moet elke onderneming haar specifieke kenmerken in een passend en evenredig bedrijfscontinuïteitsbeleid vertalen, onder meer op het vlak van de doelstellingen, de planning en de ingezette middelen voor de verwezenlijking ervan.

2.2. *Ratione materiae*

De gezonde beheerpraktijken moeten het mogelijk maken het hoofd te bieden aan ernstige niet-geplande bedrijfsonderbrekingen als gevolg van, onder andere, computerpannes, computervirussen en cybercriminaliteit, van ongevallen, ernstige sociale onrust, bomalarm, fraude, sabotage, terrorisme en natuurrampen, alsook van het uitvallen van nutsvoorzieningen (telecommunicatie, elektriciteit, aardgas, water, …).

Oorlogsdaden en gelijktijdig tegen de onderneming gerichte terroristische aanslagen op meerdere van elkaar verwijderde locaties, alsook de snelle en grootschalige verspreiding van dodelijke besmettelijke ziekten vallen buiten het toepassingsgebied. Ook door de onderneming geplande onderbrekingen van haar dienstverlening en haar activiteiten waarvan zij de cliënten, de gebruikers of andere geïnteresseerden op de hoogte heeft gebracht (bv. wegens verhuizing of onderhoudswerkzaamheden aan haar infrastructuur), blijven buiten beschouwing.

Onverminderd de specifieke kenmerken van elke onderneming, houdt de bedrijfscontinuïteitsplanning rekening met scenario's zoals:

- de volledige of gedeeltelijke vernietiging en/of onbereikbaarheid van de bedrijfsgebouwen;
- de onbeschikbaarheid van
    - kritieke bedrijfsfuncties en systemen (geïnformatiseerd of niet);
    - personen die belast zijn met de effectieve leiding van de onderneming;
    - kritieke *knowhow* en personeel dat een sleutelrol vervult;
- de tekortkomingen met betrekking tot de vertrouwelijkheid, de integriteit of de beschikbaarheid van gegevens;
- de beschadiging of het uitvallen van belangrijke infrastructuur (IT, transport, …) of nutsvoorzieningen;
- het wegvallen van belangrijke tegenpartijen en dienstverleners.

De volgende elementen worden, waar nodig, in de planning betrokken:

- de centrale en gedecentraliseerde bedrijfseenheden, alsook buitenlandse vestigingen van de onderneming die van kritiek belang zijn voor de werking van de Belgische vestiging, of vice versa;
- de ondersteunende functies;
- de centrale en gedecentraliseerde ICT-systemen (met inbegrip van de verschillende diensten die door cloud computing kunnen worden aangeboden), de gegevensbanken en de software;
- de tele- en datacommunicatiekanalen, met bijzondere aandacht voor de verbindingen met financiële markten, multilaterale handelsfaciliteiten, centrale tegenpartijen, verrekenings- en vereffeningsinstellingen, belangrijke tegenpartijen en distributienetwerken;
- de aan derde dienstverleners uitbestede diensten.

3. Vastlegging van een bedrijfscontinuïteitsbeleid door de onderneming

Elke onderneming beschikt over een aangepaste bedrijfscontinuïteitsstrategie en een dito beleid. Rekening houdend met de aard, de omvang en de complexiteit van haar activiteiten, moet zij haar organisatie zo opzetten dat zij, bij een ernstige en niet-geplande onderbreking van haar activiteiten, haar kritieke bedrijfsfuncties kan handhaven of zo spoedig mogelijk kan herstellen, en zij haar normale dienstverlening en de normale uitoefening van haar activiteiten binnen een redelijke tijdspanne kan hervatten.

De hoogste leiding van de onderneming (in beginsel de raad van bestuur) keurt deze strategie en de krachtlijnen van het bedrijfscontinuïteitsbeleid goed, en ziet erop toe dat de met de effectieve leiding belaste personen de nodige stappen ondernemen om deze nader uit te werken en toe te passen. Periodiek en minstens eenmaal per jaar brengt de effectieve leiding verslag uit aan de hoogste leiding over de bedrijfscontinuïteit in het algemeen en over de werking en de doeltreffendheid van de bedrijfscontinuïteitsplanning en het BCP in het bijzonder. In voorkomend geval wordt één lid van de effectieve leiding met de coördinatie en de rapportering belast.

De strategie en de krachtlijnen van het beleid hebben vooral betrekking op de volgende punten:

- de sensibilisering op alle niveaus van de onderneming over het belang van de bedrijfscontinuïteit en van het BCP;
- de identificatie van de kerndienstverlening en van de kritieke bedrijfseenheden, -functies en -systemen;
- de bepaling van de voor de onderneming aanvaardbare maximumduur om haar kritieke bedrijfseenheden, -functies en -systemen opnieuw beschikbaar te stellen na een niet-geplande onderbreking;
- de bepaling van de aanvaardbaar geachte vermindering van de dienstverlening aan derden en van de tijdshorizon voor de hervatting van de normale dienstverlening en bedrijfsactiviteit na een niet-geplande onderbreking;
- de bepaling van de verantwoordelijkheden en de rapporteringslijnen inzake bedrijfscontinuïteit;
- de toepassing van preventieve en risicobeperkende maatregelen;
- de toekenning van het budget en de middelen.

De met de interne auditfunctie belaste personen nemen de werking en de toepassing van het bedrijfscontinuïteitsbeleid en van het BCP van de onderneming op in hun auditplanning en -werkzaamheden en evalueren die. Daartoe worden passende auditprogramma's en -technieken ingezet.

4. Invulling van het bedrijfscontinuïteitsbeleid

4.1. *Analyse van de discontinuïteitsrisico's en van de kwetsbaarheid van de onderneming*

Aan de hand van voornoemde beginselen analyseert de onderneming de discontinuïteitsrisico's en de verschillende scenario's die op haar van toepassing zijn. Waar mogelijk, kwantificeert zij in een bedrijfsimpactanalyse de gevolgen van de realisatie van de onderkende risico's en scenario's voor de cliënten, de tegenpartijen, de markten en het personeel, alsook voor de interne dienstverlening, de financiële situatie of de reputatie van de onderneming.

4.2. *Uitwerking van de continuïteits- en herstelmaatregelen*

De onderneming werkt, in functie van de vastgelegde strategie en de krachtlijnen als bedoeld in punt 3, gedetailleerde bedrijfscontinuïteitsmaatregelen uit om de nagestreefde doelstellingen te kunnen verwezenlijken.

Het BCP is hiervan het concrete resultaat en omvat dus de maatregelen, procedures, informatie, enz. die nodig zijn om de gevolgen van een ernstige en niet-geplande onderbreking van de activiteiten op te vangen en te beheren.

Het BCP, dat doorgaans verschillende deelplannen telt, moet worden opgesteld in het licht van de aard, de omvang en de complexiteit van de activiteiten, moet voldoende gedetailleerd en gebruiksvriendelijk zijn, moet aan de betrokken medewerkers worden meegedeeld en moet op verschillende locaties worden bijgehouden, ook op plaatsen die niet als kritiek worden beschouwd.

Het BCP bevat de volgende onderdelen:

(a) crisismanagement: besluitvormingsstructuren (bv. crisismanagementcomité) en procedures die in werking treden bij ernstige niet-geplande onderbrekingen van de activiteiten, met vermelding van alle personen die daarin een rol spelen, en van hun respectieve verantwoordelijkheden, van de rapporteringswijze en van de prioriteiten.

(b) communicatie: procedures en respectieve verantwoordelijkheden voor de communicatie met het personeel, de toezichthouders (FSMA, NBB, …), de media, de markten, de belangrijke tegenpartijen en de cliënten.

(c) recuperatie van kritieke informatie: behoud of recuperatie van alle kritieke informatie, zowel op papier als op IT-drager (bv. documenten en kritieke contracten) door middel van kopie, scanning, bewaring op andere locaties (eventueel met de mogelijkheid tot raadpleging op afstand), … Uiteraard geldt dit ook voor het BCP en voor de overeenkomsten en de *service level agreements* met dienstverleners die bij een onderbreking tussenbeide moeten komen, alsook voor de nodige procedureboeken, de ICT-licenties en de handleidingen.

(d) menselijk potentieel en uitrusting: onverminderd de uitvoering van de toepasselijke maatregelen om het personeel op passende wijze te beschermen bij een ramp, vastlegging van de manier waarop kritiek personeel op de afgesproken locaties kan worden gebracht en daar kan functioneren (kantoren, uitrusting en bevoorrading, …). Ook het beroep op interim-medewerkers of externe specialisten kan in dit punt aan bod komen.

(e) herstel van de kritieke bedrijfsfuncties: procedures voor de verschillende bedrijfsfuncties en –processen die, bij een onderbreking van de activiteiten, moeten worden behouden of hersteld overeenkomstig de ter zake vastgestelde vereisten (zie punt 3). Deze planning moet eenvoudig, duidelijk en gestructureerd (*checklists,* stapsgewijze procedures) zijn, zodat hij ook kan worden begrepen en uitgevoerd door personen die ter zake niet noodzakelijk alle deskundigheid bezitten. Ook dient rekening te worden gehouden met de mogelijke vervlechting van bedrijfsactiviteiten, met kritieke knooppunten (zogenaamde *single points of failure)* en met de afhankelijkheid van andere interne of externe partijen. Het kan ook aangewezen zijn om te voorzien in manuele procedures voor het geval de ICT-ondersteuning van de onderneming niet beschikbaar is.

Indien de aard, de omvang en de complexiteit van de activiteiten dit vereist, dient de onderneming te beschikken over de mogelijkheid om uit te wijken naar één of meer uitwijkcentra op afstand (voor de kenmerken van een uitwijkcentrum en de afstand ten aanzien van het bedrijfscentrum, zie *mutatis mutandis* punt (f) en Bijlage 1);

(f) Informatie- en telecommunicatietechnologie ("ICT"): procedures die aangeven wanneer, waar, hoe en in welke volgorde kritieke ICT-systemen en -bestanden worden hersteld of opnieuw aangemaakt bij verlies, beschadiging of vernietiging. Aangezien de aanwezigheid van kritieke medewerkers bij een niet-geplande onderbreking niet kan worden gegarandeerd, moeten deze procedures zodanig zijn opgesteld dat zij ook door andere, in voorkomend geval, minder ervaren personen kunnen worden uitgevoerd.

Indien de aard, de omvang en de complexiteit van de activiteiten dit vereist, voorziet het plan in de uitrusting van één of meer beveiligde data-uitwijkcentra op afstand voor de kritieke ICT-systemen met de volgende kenmerken:

i. het uitwijkcentrum is gelegen op een toereikende geografische afstand van het ICT-bedrijfscentrum van de onderneming; die afstand wordt verantwoord op basis van een objectieve risicoanalyse die wordt uitgevoerd in het licht van de in Bijlage 1 vermelde criteria;

ii. in het uitwijkcentrum is voldoende plaats voor hardware en personeel;

iii. de nodige apparatuur, bestanden, software en informatie zijn permanent beschikbaar om het ICT-herstel binnen de vooropgestelde vereisten te realiseren;

iv. het uitwijkcentrum is uitgerust met de noodzakelijke ICT-randapparatuur, zoals koelsystemen, stroomvoorziening, monitoringsystemen, …;

v. er zijn aangepaste telecommunicatie- en nutsvoorzieningen beschikbaar die volledig losstaan van de voorzieningen die door het ICT-bedrijfscentrum van de onderneming worden gebruikt;

vi. de fysieke en ICT-beveiligingsmaatregelen moeten zowel tijdens de onderbreking als in de herstelfase voldoende worden gehandhaafd.

Dit plan dient tevens twee essentiële begrippen te definiëren die enerzijds de opstarttermijn van de activiteiten (RTO = Recovery Time Objective) en anderzijds de hoeveelheid aanvaardbaar gegevensverlies gelinkt aan een incident (RPO = Recovery Point Objective) nader bepalen.

4.3. *Testen, evaluatie en aanpassing*

(a) testen

De doelmatigheid van het BCP en van de onderdelen ervan, inzonderheid van de uitwijkcentra op afstand, wordt nagegaan aan de hand van aangepaste testen waarvan de inhoud, de diepgang en de frequentie evenredig zijn met het belang, de veranderlijkheid en de complexiteit van de geteste elementen. Belangrijke en complexe plannen waarvan de tenuitvoerlegging handelingen en reflexen inhoudt die veel oefening vergen, worden minstens éénmaal per jaar getest. Voor onderdelen van het plan die van kritiek belang zijn, kan die frequentie hoger liggen.

Deze testen strekken er ook toe de paraatheid van het personeel en de bewustwording van het belang van de bedrijfscontinuïteit binnen de onderneming aan te scherpen, en stellen het personeel in staat om de taken waarmee het tijdens een ernstige niet-geplande onderbreking is belast, te leren kennen en uit te voeren.

De testen zijn voldoende relevant ten aanzien van de geteste hypotheses en scenario's, onder meer wat de omstandigheden en de activiteitenvolumes betreft.

De testen en de resultaten worden gedocumenteerd en geanalyseerd. Waar nodig, leiden zij tot de aanpassing van het bedrijfscontinuïteitsbeleid en van het BCP.

(b) wijzigingen

Betekenisvolle wijzigingen die de onderneming in haar organisatie, dienstverlening, activiteitenprogramma en ICT aanbrengt, zijn aanleiding om het passende karakter van de bestaande bedrijfscontinuïteitsvoorzieningen en het BCP te onderzoeken en om deze, zo nodig, aan te passen met toepassing van voornoemde regels.

De betrokken kritieke bedrijfseenheden en -functies zorgen voor een regelmatig nazicht van hun continuïteitsvoorzieningen en hun gedetailleerde procedures, zodat deze kunnen worden aangepast aan de wijzigingen die hun werking beïnvloeden (personeel, communicatiemiddelen, systemen, …).

5. ***Betrokkenheid van externe dienstverleners***

De onderneming die, voor sommige onderdelen van de bedrijfscontinuïteit, een beroep doet op externe dienstverleners, neemt alle redelijke stappen om zich ervan te verzekeren dat de afgesproken dienstverlening beschikbaar is wanneer dit nodig is, bijvoorbeeld door te zorgen voor een passende geografische afstand tussen de uitwijkcentra en de bedrijfscentra (zie Bijlage 1), of nog door capaciteitsgaranties op te nemen in de uitbestedingsovereenkomst. Als tal van ondernemingen binnen de sector een beroep doen op dezelfde dienstverlener, kan dat bij rampen immers de kwaliteit en de beschikbaarheid van zijn dienstverlening in het gedrang brengen.

Voor deze en andere punten waarmee rekening dient te worden gehouden in geval van uitbesteding, wordt ook verwezen naar de FSMA-circulaire over de gezonde beheerpraktijken bij uitbesteding, die beschikbaar is op de FSMA-website http://www.fsma.be/nl/Supervision/finbem/bo/circmedprak/vvb.aspx

⁂

Bijlage 1

Criteria voor de bepaling van de minimumafstand tussen

de ICT-centra en de uitwijkcentra

Gezien de grote verscheidenheid aan risicoprofielen dient elke financiële instelling zelf haar risico's te evalueren, om zo de gepaste minimumafstand te kunnen bepalen tussen haar ICT-centrum en haar uitwijkcentrum voor kritieke ICT-systemen. Daarbij dienen minstens de hieronder vermelde punten in aanmerking te worden genomen:

- de mogelijke vernietiging van volledige *datacenters* en bedrijfscentra, inclusief het verlies van sleutelpersonen;
- de geologische en meteorologische gevaren (overstromingen, aardbevingen, enz.); alle *datacenters* in eenzelfde, aan overstromingen blootgestelde zone vestigen zou bijvoorbeeld onaanvaardbaar zijn;
- de omgevingsrisico's (nabijheid van industriële activiteiten met een hoog risicoprofiel, luchthavens, ambassades, overheidsinstellingen en militaire installaties, enz.); zo moet er bijvoorbeeld een grotere afstand tussen de *datacenters* zijn indien één ervan is gelegen in de buurt van een kerncentrale of een mogelijk doelwit voor terroristische aanslagen, zoals de vestigingen van internationale instellingen; ook voor *datacenters* die zich in grote agglomeraties en in zones met een gevaarlijke industriële activiteit bevinden, moet, gelet op dat risico, een grotere veiligheidsafstand worden ingebouwd;
- de mogelijke onbereikbaarheid van de *datacenters* en de bedrijfsgebouwen door sociale onrust, ontruimingen, veiligheidsperimeters, vernietiging of oververzadiging van de toegangswegen; er moet worden vermeden dat, wanneer zich een incident voordoet in het primaire ICT-centrum, het uitwijkcentrum enkel bereikbaar is via toegangswegen die versperd dreigen te raken;
- de schade door een terroristische aanslag op kritieke infrastructuur of op een kritieke financiële instelling of haar omgeving;
- de schade aan de onmiddellijke omgeving en aan de nutsvoorzieningen; in dit verband is het van essentieel belang dat de ICT-centra en de uitwijkcentra een beroep doen op leveranciers van nutsvoorzieningen zonder *"single points of failure*" die geografisch voldoende ver van elkaar zijn verwijderd om niet door eenzelfde plaatselijk incident te worden getroffen; in landelijke gebieden waar het netwerk van nutsvoorzieningen minder vertakt en redundant is, zou de minimale veiligheidsafstand tussen de *datacenters* groter moeten zijn dan in de agglomeraties of industriezones met een wijdvertakt en redundant netwerk.

⁂