Brussel, 10 maart 2005

Circulaire in verband met gezonde beheerspraktijken inzake de bedrijfscontinuïteit van financiële instellingen

PPB/D.256

1. Verantwoording en definities

Kredietinstellingen, verzekeringsondernemingen, beleggingsondernemingen[1] en beheer-vennootschappen van instellingen voor collectieve belegging moeten beschikken over een voor hun activiteit passende organisatie.[2]

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

Een aangepast bedrijfscontinuïteitsbeleid is in dit verband een noodzakelijk instrument om deze doelstellingen te realiseren.

Het laat zich aanzien dat het thema van de bedrijfscontinuïteit ook op de agenda van internationale overlegfora en regelgevers komt, waardoor in de toekomst geharmoniseerde regels tot stand kunnen komen. Dit belet niet dat de Belgische financiële instellingen nu reeds werk maken van hun bedrijfscontinuïteitsbeleid en maatregelen nemen om hun organisatie op dat vlak te vervolledigen of te verbeteren.

Deze circulaire somt een aantal criteria op – vertaald als gezonde beheerspraktijken – aan de hand waarvan de CBFA het bedrijfscontinuïteitsbeleid van de financiële instellingen onder haar toezicht zal toetsen.

---

[1] Hierna wordt onder "beleggingsondernemingen" begrepen, de beleggingsondernemingen als bedoeld in artikel 47 van de wet van 6 april 1995, evenals de vennootschappen voor beleggingsadvies (artikel 119 van de wet van 6 april 1995) en de derivatenspecialisten (artikel 45, 10°, van de wet van 6 april 1995 en het KB van 28 januari 2004).

[2] Zie artikel 20 van de wet van 22 maart 1993 (kredietinstellingen), artikel 14bis van de Wet van 9 juli 1975 (verzekeringsondernemingen), artikel 62 en 124 van de wet van 6 april 1995 (beleggingsondernemingen, vennootschappen voor beleggingsadvies) en artikel 9 van het KB van 28 januari 2004 (derivatenspecialisten). Voor de beheervennootschappen van instellingen voor collectieve belegging, zie artikel 153, §1, van de wet van 20 juli 2004 betreffende bepaalde vormen van collectief beheer van beleggingsportefeuilles.

In deze circulaire wordt verstaan onder:

bedrijfscontinuïteit:	de doelstelling om de dienstverlening en activiteiten in alle omstandigheden een ongestoord verloop te laten kennen;
bedrijfscontinuïteitsbeleid:	het vastleggen van een strategie inzake bedrijfscontinuïteit en van een uitvoeringsbeleid dat erop is gericht om alle redelijke maatregelen te nemen om de bedrijfscontinuïteit te verzekeren;
bedrijfscontinuïteitsplanning:	het plannings- en voorbereidingsproces dat – in uitvoering van het bedrijfscontinuïteitsbeleid – uitmondt in een bedrijfscontinuïteitsplan;
bedrijfscontinuïteitsplan, afgekort “BCP”:	een verzameling van procedures en documentatie die worden ontwikkeld en in een coherent geheel samengebracht en ter beschikking gehouden voor het geval zich een niet-geplande onderbreking voordoet.

2. Toepassingsgebied

2.1. *Ratione personae*

De gezonde beheerspraktijken zijn van toepassing op de kredietinstellingen, de verzekeringsondernemingen, de beleggingsondernemingen en de beheervennootschappen van instellingen voor collectieve belegging naar Belgisch recht. Ze zijn ook van toepassing op de Belgische bijkantoren van kredietinstellingen, verzekeringsondernemingen, beleggings-ondernemingen en beheervennootschappen van 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 in de concrete invulling van hun bedrijfscontinuïteitsbeleid. De onderneming moet in dergelijk geval aantonen dat de groepsgewijze organisatie geen afbreuk doet aan de deugdelijkheid van haar bedrijfscontinuïteitsbeleid.

De gezonde beheerspraktijken zijn relevant voor zowel grote als kleine instellingen, hoewel de gevolgen van onderbrekingen voor elk bedrijf erg verschillend kunnen zijn. Daarom moet elke instelling haar specifieke kenmerken vertalen in een passend en evenredig bedrijfscontinuïteitsbeleid, onder meer wat betreft de doelstellingen, de planning en de ingezette middelen om dit te verzekeren.

De CBFA verwacht dat de instellingen die door het Comité voor Financiële Stabiliteit (“CFS”) worden beschouwd als kritiek voor de goede werking van het Belgisch financieel systeem (betalingsverkeer, verrekening en vereffening), ook de specifieke CFS-aanbevelingen ten uitvoer brengen.

2.2. *Ratione materiae*

De gezonde beheerspraktijken richten zich op ernstige niet-geplande onderbrekingen van het bedrijf als gevolg van, onder andere, computerpannes, computervirussen en cybercriminaliteit, van ongevallen, omvangrijke sociale onrust, bomalarm, fraude, sabotage, terrorisme, natuurrampen, alsook van het uitvallen van nutsvoorzieningen (telecommunicatie, elektriciteit, aardgas, water,…).

Vallen buiten het toepassingsgebied, daden van oorlog en gelijktijdige tegen de onderneming gerichte terroristische aanslagen op meerdere van elkaar verwijderde locaties, evenals de snelle, grootschalige verspreiding van besmettelijke dodelijke ziekten. Blijven ook buiten beschouwing, de onderbrekingen van de dienstverlening en de activiteit die de onderneming zelf heeft gepland en met de cliënten, gebruikers of andere geïnteresseerden heeft gecommuniceerd (bijvoorbeeld wegens verhuizing, onderhoudswerkzaamheden aan haar infrastructuur).

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

- de gehele of gedeeltelijke vernietiging en/of onbereikbaarheid van bedrijfsgebouwen;
- de onbeschikbaarheid van
  - kritieke bedrijfsfuncties en systemen;
  - personen die de effectieve leiding van de onderneming in handen hebben;
  - kritieke *know how* en personeel dat een sleutelrol vervult;
- de verdwijning of beschadiging van gegevens;
- schade aan of het uitvallen van belangrijke infrastructuur (IT, transport,…) of nutsvoorzieningen;
- het wegvallen van belangrijke wederpartijen en dienstverleners.

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

- centrale en gedelocaliseerde bedrijfseenheden, alsook buitenlandse vestigingen die van kritiek belang zijn voor de werking van de Belgische vestiging, of vice versa;
- ondersteunende functies;
- centrale en gedecentraliseerde ICT-systemen, gegevensbanken en software;
- tele- en datacommunicatiekanalen, met bijzondere aandacht voor verbindingen met financiële markten, multilaterale handelsfaciliteiten, centrale tegenpartijen, verrekenings- en vereffeningsinstellingen, belangrijke wederpartijen en distributienetwerken;
- aan derde dienstverleners uitbestede diensten.

3. <u>Vastlegging van een bedrijfscontinuïteitsbeleid door de instelling</u>

Elke instelling beschikt over een aangepaste strategie en beleid inzake haar bedrijfscontinuïteit. Rekening houdend met de aard, schaal en complexiteit van haar bedrijf, moet zij haar organisatie zo opzetten dat, in geval zich een ernstige en niet-geplande onderbreking van het bedrijf voordoet, haar kritieke bedrijfsfuncties kan behouden of zo spoedig mogelijk herstellen en haar normale dienstverlening en activiteit binnen een redelijke tijdspanne kan hervatten.

De hoogste leiding van de instelling (in de regel de raad van bestuur) keurt deze strategie en de krachtlijnen van het bedrijfscontinuïteitsbeleid goed en ziet erop toe dat de personen belast met de uitvoerende leiding de nodige stappen ondernemen om deze nader uit te werken en toe te passen.

Periodiek en minstens eenmaal per jaar brengt de uitvoerende leiding verslag uit aan de hoogste leiding over de bedrijfscontinuïteit in het algemeen en over de werking en doeltreffendheid van de bedrijfscontinuïteitsplanning en het BCP in het bijzonder. In voorkomend geval wordt één lid van de uitvoerende leiding belast met coördinatie en rapportering.

De strategie en de krachtlijnen van het beleid hebben o.a. betrekking op:

- sensibiliseren op alle niveau's van de onderneming over het belang van de bedrijfscontinuïteit en van het BCP;
- identificeren van de kerndienstverlening en van de kritieke bedrijfseenheden, -functies en –systemen;
- bepalen van de maximumduur die de instelling aanvaardt om haar kritieke bedrijfseenheden, -functies en -systemen terug beschikbaar te stellen na een niet-geplande onderbreking;
- vastleggen van de aanvaardbaar geachte vermindering van de dienstverlening ten aanzien van derden en de tijdshorizon voor de hervatting van de normale dienstverlening en bedrijfsactiviteit na een niet-geplande onderbreking;
- bepalen van de verantwoordelijkheden en rapporteringslijnen inzake bedrijfscontinuïteit;
- toepassen van preventieve en risicoreducerende maatregelen;
- toekennen van het budget en de middelen.

De interne auditfunctie neemt de werking en de toepassing van het bedrijfscontinuïteitsbeleid en van het BCP van de onderneming op in haar auditplanning en –werkzaamheden en evalueert die. Daartoe worden passende auditprogramma's en –technieken ingezet.

4. Invulling van het bedrijfscontinuïteitsbeleid

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

Aan de hand van de uitgangspunten zoals hierboven besproken, analyseert de instelling de discontinuïteitsrisico's en de verschillende scenario's die op de onderneming van toepassing zijn. Waar mogelijk worden in een bedrijfsimpactanalyse de gevolgen gekwantificeerd van de realisatie van de onderkende risico's en scenario's ten aanzien van de cliënten, wederpartijen, markten, personeel, interne dienstverlening, van de financiële situatie of de reputatie van de instelling.

4.2. *Uitwerking van de continuïteits- en herstelmaatregelen*

De instelling werkt – in functie van de vastgelegde strategie en krachtlijnen zoals bedoeld in punt 3 – gedetailleerde bedrijfscontinuïteitsmaatregelen uit om de nagestreefde doelstellingen te kunnen bereiken.

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

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

Het BCP bevat de volgende onderdelen:

(a) crisis management: beslissingsstructuren (bv. crisis management comité) en procedures die in werking treden in geval van ernstige niet-geplande onderbrekingen, met aanduiding van alle personen die daarin een rol spelen en van hun respectieve verantwoordelijkheden, rapportering en prioriteiten.

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

(c) recuperatie van kritieke documentatie: behoud of recuperatie van alle kritieke documenten en contracten door middel van kopie, scanning, bewaring op andere locaties (met desgevallend mogelijkheid tot raadpleging op afstand),… Uiteraard geldt dit ook voor het BCP en voor overeenkomsten en *service level agreements* met dienstverleners die in geval van onderbreking moeten tussenkomen, alsook voor de nodige procedureboeken, ICT-licenties en handleidingen.

(d) menselijk potentieel en uitrusting: onverminderd de uitvoering van de toepasselijke maatregelen om het personeel in het geval van een ramp passend te beschermen, vastleggen van de manier waarop kritiek personeel op de afgesproken locaties kan worden gebracht en functioneren (kantoren, uitrusting en bevoorrading,…). Ook het beroep op interim-medewerkers of externe specialisten kan hieronder vallen.

(e) herstel van de kritieke bedrijfsfuncties: procedures voor de verschillende bedrijfsfuncties en –processen die ingeval van onderbreking moeten worden behouden of hersteld overeenkomstig de vereisten die terzake zijn vastgelegd (zie punt 3). Deze planning kan door zijn eenvoud, duidelijkheid en structuur (*check lists, step-by-step* procedures) ook worden begrepen en uitgevoerd door personen die terzake niet noodzakelijk alle deskundigheid bezitten. Ook wordt rekening gehouden met mogelijke vervlechting van bedrijfsactiviteiten, met kritieke knooppunten (zogenaamde *single points of failure)* en met afhankelijkheid van andere interne of externe partijen. Het kan ook aangewezen zijn om manuele procedures te voorzien voor het geval de ICT-ondersteuning van de onderneming niet beschikbaar is.

Indien de aard, de schaal en de complexiteit van de activiteit dit vereist, dient de instelling 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 ingeval van verlies, beschadiging of vernietiging. Gezien de aanwezigheid van kritieke medewerkers bij een ongeplande onderbreking niet kan worden gegarandeerd, zijn deze procedures zodanig opgesteld dat ze ook door andere, in voorkomend geval, minder ervaren personen kunnen worden uitgevoerd.

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

i. een uitwijkcentrum is gelegen op een betekenisvolle geografische afstand van het ICT-bedrijfscentrum van de onderneming; de afstand wordt op basis van een objectieve risicoanalyse verantwoord met aandacht voor de criteria opgenomen in Bijlage 1;
ii. voldoende plaats voor hardware en personeel;
iii. beschikbaarheid van apparatuur, bestanden, software en informatie, die nodig zijn om het ICT-herstel binnen de vooropgestelde vereisten te realiseren;
iv. beschikbaarheid van noodzakelijke ICT-randapparatuur zoals koelsystemen, stroomvoorziening, monitoringsystemen,…;
v. beschikbaarheid van aangepaste telecommunicatie- en nutsvoorzieningen die ontdubbeld zijn van die gebruikt door het ICT-bedrijfscentrum van de onderneming;
vi. de fysieke en ICT-beveiligingsmaatregelen moeten tijdens de onderbreking en in de herstelfase op een voldoende wijze worden gehandhaafd.

4.3. *Testen, evaluatie en aanpassing*

(a) testen

De doelmatigheid van het BCP en van zijn onderdelen, inzonderheid van de uitwijkcentra op afstand, wordt nagegaan aan de hand van aangepaste testen waarvan de inhoud, diepgang en frequentie evenredig is met hun belang, veranderlijkheid en complexiteit. Belangrijke en complexe plannen waarvan de handelingen en reflexen veel oefening vergen, worden minstens éénmaal per jaar getest. Hogere frequenties kunnen gelden voor onderdelen van plannen die van kritiek belang zijn.

Deze testen beogen ook de paraatheid van het personeel en de bewustwording van het belang van de bedrijfscontinuïteit binnen de instelling aan te scherpen en stellen het personeel in staat om de taken die het tijdens een ernstige niet-geplande onderbreking zijn toebedeeld, te leren kennen en uitvoeren.

De testen hebben voldoende relevantie ten aanzien van de geteste hypotheses en scenario's, onder meer wat betreft omstandigheden en activiteitsvolumes.

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

(b) wijzigingen

Betekenisvolle wijzigingen die de instelling aanbrengt aan haar organisatie, dienstverlening, activiteitenprogramma en ICT, zijn aanleiding om de aangepastheid van de bestaande bedrijfscontinuïteitsvoorzieningen en het BCP te onderzoeken en om dit zo nodig, met toepassing van de hierboven beschreven regels, aan te passen.

De betrokken kritieke bedrijfseenheden en -functies staan in voor een regelmatig nazicht van hun continuïteitsvoorzieningen en gedetailleerde procedures om deze aan te passen aan de wijzigingen die zich in hun werking voordoen (personeel, communicatiemiddelen, systemen,…).

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

De instelling die voor 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 van de uitwijkcentra ten aanzien van de bedrijfscentra (zie Bijlage 1), of nog door in de uitbestedingsovereenkomst capaciteitsgaranties op te nemen. Immers, een sterke sectorale concentratie van beroep op eenzelfde dienstverlener kan in geval van rampen de kwaliteit en de beschikbaarheid van diens dienstverlening in het gedrang brengen.

Voor deze en andere bekommernissen in geval van uitbesteding, zie ook de CBFA-circulaire over de gezonde beheerspraktijken bij uitbesteding.[3]

6. ***Evaluatie van het bestaande bedrijfscontinuïteitsbeleid, –planning en streefdata.***

De CBFA verwacht van de instellingen dat zij hun bedrijfscontinuïteitsbeleid tegen einde 2005 evalueren in het licht van de gezonde beheerspraktijken vermeld in deze circulaire en bepalen welke maatregelen desgevallend worden genomen, en binnen welke termijn, om hun organisatie terzake aan te passen.

De technische invulling en realisatie van bepaalde aspecten van het bedrijfscontinuïteitsplan kunnen belangrijke organisatorische ingrepen of termijnen voor tenuitvoerlegging (vb. uitrusting uitwijkcentra) vergen. De betrokken instellingen maken voor deze aspecten een programma op om hun doelstellingen binnen een redelijke termijn – te beoordelen in het licht van de aard, schaal en complexiteit van hun bedrijf – te halen. Indien dit programma termijnen hanteert, die einde 2007 overschrijden, dient dit met de CBFA te worden besproken. Overigens vormt dergelijke spreiding van tenuitvoerlegging geen beletsel voor de beoordeling door de CBFA van het bedrijfscontinuïteitsbeleid als geheel op basis van de onderhavige beheerspraktijken.

⁂

[3] Voor kredietinstellingen en beleggingsondernemingen, zie circulaire PPB 2004/5 van 22 juni 2004.

Bijlage 1

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

Gezien de grote verscheidenheid aan risicoprofielen dient elke financiële instelling zelf haar risico's te evalueren en op grond hiervan de gepaste minimumafstand te bepalen tussen haar ICT-centrum en haar uitwijkcentrum voor kritieke ICT-systemen. Daarbij dienen minstens de onderstaande punten in aanmerking te worden genomen:

- de mogelijke vernietiging van volledige *datacenters* en bedrijfscentra, met inbegrip van 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 hoog risicoprofiel, luchthavens, ambassades, overheidsinstellingen en militaire installaties, enz.); zo moet er bijvoorbeeld een grotere afstand zijn tussen de *datacenters* indien één ervan is gelegen in de buurt van een kerncentrale of van een mogelijk doelwit voor terroristische aanslagen, zoals de vestigingen van internationale instellingen; ook voor *datacenters* die zich in grote agglomeraties bevinden en in zones met een gevaarlijke industriële activiteit moet, gelet op dat risico, een grotere veiligheidsafstand worden ingebouwd;

- de mogelijke onbereikbaarheid van de *datacenters* en bedrijfsgebouwen door sociale onrust, ontruimingen, veiligheidsperimeters, vernietiging of oververzadiging van de toegangswegen; er moet worden vermeden dat het uitwijkcentrum enkel bereikbaar is via een toegangsweg die versperd dreigt te zijn wanneer zich een incident voordoet in het primaire ICT-centrum;

- de schade door een terroristische aanslag op kritieke infrastructuur of tegen een kritieke financiële instelling of haar omgeving;

- de schade aan de onmiddellijke omgeving en aan de nutsvoorzieningen; in dit kader is het van essentieel belang dat de ICT- en uitwijkcentra nutsvoorzieningen zonder *"single points of failure"* benutten en die geografisch voldoende 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.

⁂