FSMA
AUTORITÉ DES SERVICES ET MARCHÉS FINANCIERS

Circulaire

FSMA_2016_03 du 1/03/2016

Saines pratiques de gestion visant à assurer la continuité des activités des entreprises réglementées

Champ d'application :

La présente circulaire est applicable aux :
- sociétés de gestion de portefeuille et de conseil en investissement de droit belge ;
- sociétés de gestion d'organismes de placement collectif (alternatifs) de droit belge ;
- succursales belges des sociétés de gestion de portefeuille et de conseil en investissement et des sociétés de gestion d'organismes de placement collectif (alternatifs) qui relèvent du droit d'un Etat non membre de l'Union Européenne.

Résumé/Objectifs :

La présente circulaire énumère, sous la forme de saines pratiques de gestion, un certain nombre de critères sur la base desquels la FSMA examinera la politique de continuité mise en place par les entreprises réglementées soumises à son contrôle.

Structure :

1. Justification et définitions
2. Champ d'application
3. Mise en place par chaque établissement d'une politique de continuité des activités
4. Eléments de la politique de continuité des activités
5. Implication des prestataires de services externes

Annexe 1 - Critères pour la détermination de la distance minimale entre les centres ICT et les centres de secours

1. Justification et définitions

Les sociétés de gestion de portefeuille et de conseil en investissement et les sociétés de gestion d'organismes de placement collectif (alternatifs) doivent disposer d'une organisation appropriée à leurs activités.[1]

Cette condition d'agrément implique notamment que les entreprises concernées mettent en œuvre tous les moyens raisonnables pour assurer leurs prestations de services et exercer leurs activités sans interruption. Tenant compte de la nature, de l'échelle et de la complexité de leurs activités, elles doivent plus précisément veiller à ce que leur organisation, leurs systèmes et leurs procédures soient conçus de manière telle qu'en cas d'interruption sérieuse et non planifiée de leurs activités, elles puissent continuer à remplir leurs obligations résultant de leur statut de contrôle et préserver les intérêts et les droits de leurs clients.

Une politique adéquate en matière de continuité des activités constitue, dans ce cadre, un instrument nécessaire à la réalisation de ces objectifs.

La présente circulaire énumère, sous la forme de saines pratiques de gestion, un certain nombre de critères sur la base desquels la FSMA examinera la politique de continuité mise en place par les entreprises réglementées soumises à son contrôle.

Celle-ci remplace, avec effet immédiat, la circulaire PPB 2005/2 concernant les saines pratiques de gestion visant à assurer la continuité des institutions financières pour ce qui est des entreprises réglementées entrant dans son champ d'application.

[1] Voir l'article 62 bis, § 3 de la loi du 6 avril 1995 relative au statut et au contrôle des entreprises d'investissement, l'article 221 de la loi du 3 août 2012 relative aux organismes de placement collectif qui répondent aux conditions de la directive 2009/65/CE et aux organismes de placement en créances, l'article 4, § 3 de l'arrêté royal du 12 novembre 2012 relatif aux sociétés de gestion d'organismes de placement collectif, l'articles 33 de la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires et 57, § 3 du règlement délégué n° 231/2013 de la Commission européenne du 19 décembre 2012 complétant la directive 2011/61/UE du Parlement européen et du Conseil en ce qui concerne les dérogations, les conditions générales d'exercice, les dépositaires, l'effet de levier, la transparence et la surveillance.

Dans cette circulaire, on entend par :

continuité des activités :	l'objectif d'assurer les prestations de services et d'exercer les activités en toutes circonstances et sans perturbation ;
politique de continuité :	l'établissement d'une stratégie en matière de continuité des activités et d'une politique de mise en œuvre visant à prendre toutes les mesures raisonnables pour assurer la continuité des activités ;
planning de continuité :	le processus de planification et de préparation qui, en exécution de la politique de continuité, se traduit en un plan de continuité ;
plan de continuité, en abrégé « BCP » :	un recueil de procédures et de documentation, développé et établi comme un ensemble cohérent, et disponible en cas de survenance d'une interruption non planifiée.

2. Champ d'application

2.1. *Ratione personae*

Les saines pratiques de gestion s'appliquent aux sociétés de gestion de portefeuille et de conseil en investissement et aux sociétés de gestion d'organismes de placement collectif (alternatifs) de droit belge. Elles sont également applicables aux succursales belges des sociétés de gestion de portefeuille et de conseil en investissement et des sociétés de gestion d'organismes de placement collectif (alternatifs) qui relèvent du droit d'un Etat non membre de l'Union Européenne.

Pour les entreprises faisant partie d'un groupe, la dimension de groupe peut jouer un rôle important dans la définition et la mise en œuvre de la politique de continuité. Dans ce cas, l'entreprise doit démontrer que l'organisation au niveau du groupe ne nuit pas au caractère adéquat de sa politique de continuité.

Les saines pratiques de gestion présentent un intérêt tant pour les grands que pour les petits établissements, bien que les conséquences d'une interruption d'activité puissent être très différentes pour chacun d'eux. C'est la raison pour laquelle il appartiendra à chaque établissement de tenir compte de ses caractéristiques spécifiques pour établir une politique de continuité, adéquate et proportionnée, notamment en ce qui concerne les objectifs, la planification et les moyens engagés pour les réaliser.

2.2. *Ratione materiae*

Les saines pratiques de gestion doivent permettre de faire face à des interruptions sérieuses et non planifiées des activités, résultant notamment de pannes informatiques, d'attaques informatiques et de cybercriminalité, d'accidents, de perturbations sociales importantes, d'alertes à la bombe, de fraudes, de sabotages, d'actes de terrorisme, de catastrophes naturelles, ainsi que de la défaillance de services d'utilité publique (télécommunications, électricité, gaz naturel, eau,…).

Ne tombent pas dans leur champ d'application les actes de guerre et les attentats terroristes dirigés simultanément contre plusieurs sites de l'entreprise installés à des endroits différents, ainsi que la prolifération rapide et à grande échelle de maladies contagieuses mortelles. Ne sont pas davantage visées les interruptions de services et d'activités que l'entreprise a planifiées et dont elle a informé les clients, les utilisateurs ou les autres personnes concernées (par exemple, en raison d'un déménagement ou de travaux d'entretien effectués à son infrastructure).

Sans préjudice des caractéristiques propres à chaque entreprise, le planning de continuité des activités tiendra compte de scénarios tels que :

- la destruction totale ou partielle et/ou l'inaccessibilité des bâtiments opérationnels ;
- l'indisponibilité
    - de fonctions et systèmes critiques (informatisés ou non) ;
    - de personnes chargées de la direction effective de l'entreprise ;
    - de savoir-faire critique ou de personnel remplissant un rôle clé ;
- les failles impactant la confidentialité, l'intégrité ou la disponibilité des données ;
- l'endommagement ou la défaillance d'infrastructures importantes (IT, transports,…) ou de services d'utilité publique ;
- la perte de contreparties ou de prestataires de services importants.

Les éléments suivants seront, le cas échéant, intégrés dans le planning :

- les entités centrales et délocalisées, ainsi que les sites étrangers de l'entreprise qui revêtent une importance critique pour le fonctionnement du site belge, ou vice versa ;
- les fonctions de support ;
- les systèmes ICT centraux et décentralisés (y compris les différents services pouvant être offerts par le cloud computing dans son ensemble), les bases de données et les logiciels ;
- les canaux de télécommunication et de transmission des données, une attention particulière étant portée aux connexions établies avec les marchés financiers, les facilités commerciales multilatérales, les contreparties centrales, les dépositaires (des fonds gérés), les contreparties importantes et les réseaux de distribution ;
- les services sous-traités à des prestataires de services tiers.

3. Mise en place par chaque établissement d'une politique de continuité des activités

Chaque établissement dispose d'une stratégie et d'une politique adéquates concernant la continuité de ses activités. Tenant compte de la nature, de l'échelle et de la complexité de ses activités, il doit plus précisément veiller à ce que son organisation soit conçue de manière telle qu'en cas d'interruption sérieuse et non planifiée de ses activités, il puisse maintenir ses fonctions critiques ou les rétablir le plus rapidement possible et puisse ainsi reprendre dans un délai raisonnable la fourniture de ses services habituels et l'exercice de ses activités normales.

La plus haute direction de l'établissement (en principe le conseil d'administration) approuve cette stratégie et les lignes de force de la politique de continuité des activités et veille à ce que les personnes chargées de la direction effective entreprennent les démarches nécessaires pour développer et appliquer celles-ci. Périodiquement et au moins une fois par an, la direction effective fait rapport à la plus haute direction sur la continuité des activités en général et sur le fonctionnement et l'efficacité du planning de continuité et du BCP en particulier. Le cas échéant, un membre de la direction effective est chargé de la coordination et du reporting.

La stratégie et les lignes de force de la politique portent notamment sur les points suivants :

- sensibiliser l'entreprise, à tous les niveaux, quant à l'importance de la continuité des activités et du BCP ;
- identifier les prestations de services cruciales et les entités, fonctions et systèmes critiques de l'entreprise ;
- déterminer la durée maximale acceptable par l'entreprise pour restaurer ses entités, fonctions et systèmes critiques après une interruption non planifiée ;
- déterminer la réduction jugée acceptable des services fournis à des tiers et le délai admis pour la reprise des services habituels et des activités normales après une interruption non planifiée ;
- déterminer les responsabilités et les lignes de reporting en matière de continuité des activités ;
- appliquer des mesures préventives, aptes à réduire les risques ;
- affecter le budget et les moyens.

Les personnes assurant la fonction d'audit interne intègrent le fonctionnement et l'application de la politique de continuité et du BCP de l'entreprise dans leur plan et leurs travaux d'audit et procèdent à leur évaluation. A cet effet, des programmes et techniques d'audit adéquats sont mis en place.

4. Eléments de la politique de continuité des activités

4.1. *Analyse des risques de discontinuité et de la vulnérabilité de l'entreprise*

Se fondant sur les principes énoncés ci-dessus, l'établissement analyse les risques de discontinuité et les différents scénarios applicables à sa situation. Il effectue, lorsque cela est possible, une analyse d'impact destinée à quantifier les conséquences de la réalisation des risques et des scénarios identifiés, que ce soit à l'égard des clients, des contreparties, des marchés et du personnel, ou sur le plan des services internes, de la situation financière ou de la réputation de l'établissement.

4.2. *Elaboration des mesures de continuité et de rétablissement*

L'établissement élabore, en fonction de la stratégie établie et des lignes de force visées au point 3, des mesures de continuité détaillées qui permettront d'atteindre les objectifs poursuivis.

Le BCP en constitue le résultat concret et comprend donc les mesures, procédures, informations, etc. qui sont nécessaires pour appréhender et gérer les conséquences d'une interruption sérieuse, non planifiée, des activités.

Le BCP, qui se subdivise généralement en plusieurs sections, doit être établi, en fonction de la nature, de l'échelle et de la complexité des activités, de manière suffisamment détaillée et conviviale. Il doit être communiqué aux collaborateurs concernés et doit être conservé à plusieurs endroits, même si ceux-ci ne sont pas considérés comme critiques.

Le BCP comprend les sections suivantes :

(a) gestion de crises : cette section traite des structures de décision (par exemple, le comité de gestion des crises) et des procédures à mettre en oeuvre en cas d'interruptions sérieuses, non planifiées, des activités. Y sont mentionnées toutes les personnes qui jouent un rôle en la matière, avec indication de leurs responsabilités respectives. Le mode de reporting et les priorités à observer sont également précisés.

(b) communication : cette section indique les procédures et responsabilités respectives sur le plan de la communication avec le personnel, les autorités de contrôle (FSMA, BNB, …), les médias, les marchés et les contreparties importantes, ainsi qu'avec les clients.

(c) récupération de l'information critique : cette section traite du maintien ou de la récupération de toutes les informations, sur support physique ou informatique (ex : documents et contrats critiques) au moyen de copies, d'un scanning, d'une conservation à d'autres endroits (avec éventuellement la possibilité d'une consultation à distance), etc. Ces mesures s'appliquent évidemment aussi au BCP et aux conventions et *service level agreements* conclus avec les prestataires de services qui doivent intervenir en cas d'interruption des activités, ainsi qu'aux livres de procédures, aux licences ICT et aux manuels requis.

(d) ressources humaines et équipements : cette section comprend, sans préjudice de l'exécution des mesures applicables pour assurer la protection adéquate du personnel en cas de catastrophe, les modalités selon lesquelles le personnel critique peut être amené et fonctionner aux endroits convenus (bureaux, équipements et approvisionnements,…). Le recours à des collaborateurs intérimaires ou à des spécialistes externes peut également être traité dans cette section.

(e) rétablissement des fonctions critiques : cette section expose les procédures applicables aux différentes fonctions et divers processus qui, en cas d'interruption des activités, doivent être maintenus ou rétablis, conformément aux exigences fixées en la matière (voir point 3). Cette planification doit être établie de manière simple, claire et structurée (listes de vérification, procédures par étapes) pour pouvoir être comprise et mise en oeuvre également par des personnes moins averties en la matière. Il convient à cet égard de tenir compte de l'imbrication possible de certaines activités, de points de défaillance critiques (dits *single points of failure)* et de la dépendance vis-à-vis d'autres parties internes ou externes. Il peut également être indiqué de prévoir des procédures manuelles pour le cas où l'infrastructure ICT de l'entreprise ne serait pas disponible.

Si la nature, l'échelle et la complexité de ses activités l'exigent, l'établissement doit disposer de la possibilité de migrer vers un ou plusieurs centres de secours situés à distance (pour les caractéristiques d'un centre de secours et la distance à laquelle il doit être situé par rapport au centre opérationnel, voir – mutatis mutandis – le point (f) et l'annexe 1).

(f) technologie de l'information et des télécommunications (« ICT ») : cette section reprend les procédures indiquant à quel moment, à quel endroit, de quelle manière et dans quel ordre les systèmes et fichiers ICT critiques sont rétablis ou recréés en cas de perte, d'endommagement ou de destruction. Comme la présence de collaborateurs critiques lors d'une interruption non planifiée ne peut être garantie, ces procédures doivent être rédigées de manière à pouvoir être mises en oeuvre également par d'autres personnes, éventuellement moins expérimentées.

Si la nature, l'échelle et la complexité des activités l'exigent, le plan prévoit l'équipement d'un ou de plusieurs « data center » de secours sécurisés pour les systèmes ICT critiques, centres opérant à distance et présentant les caractéristiques suivantes :

i. le centre de secours est situé à une distance géographique suffisante du centre ICT opérationnel de l'entreprise ; cette distance est justifiée sur la base d'une analyse objective des risques, établie à la lumière des critères énoncés à l'annexe 1 ;

iii. ii. il contient suffisamment de place pour le hardware et le personnel ; les appareils, fichiers, logiciels et informations nécessaires pour faire redémarrer l'ICT dans le cadre des exigences prévues sont disponibles en permanence ;

iv. le centre est équipé des périphériques ICT nécessaires, tels que des systèmes de refroidissement, une alimentation en électricité, des systèmes de monitoring, etc. ;

v. le centre peut recourir à des systèmes de télécommunication et à des services d'utilité publique adaptés, dédoublés de ceux utilisés pour le centre ICT opérationnel de l'entreprise ;

vi. les mesures de sécurité physique et ICT sont maintenues de manière suffisante, tant au moment de l'interruption que durant la phase de rétablissement.

Le plan doit aussi contenir deux notions essentielles qui définissent des délais acceptables de reprise des activités (RTO = Recovery Time Objective) et la quantité acceptable de perte de données liées à un incident (RPO = Recovery Point Objective).

4.3. *Tests, évaluation et adaptation*

(a) tests

L'efficacité du BCP et de ses différentes sections – en particulier celle relative aux centres de secours à distance – est contrôlée au moyen de tests appropriés dont le contenu, la profondeur et la fréquence sont proportionnels à l'importance, à la variabilité et à la complexité des éléments testés. Les plans importants et complexes, dont la mise en œuvre implique des actes et réflexes demandant beaucoup d'exercice, sont testés au moins une fois par an. Une fréquence plus élevée peut être appliquée aux sections du plan qui revêtent une importance critique.

Ces tests visent également à renforcer la disponibilité du personnel et la prise de conscience de l'importance de la continuité des activités au sein de l'établissement. Ils permettent aux membres du personnel d'apprendre à connaître et à effectuer les tâches qu'ils devront assumer en cas d'interruption sérieuse non planifiée.

Les tests sont suffisamment pertinents au regard des hypothèses et scénarios testés, notamment en ce qui concerne les circonstances et les volumes d'activité.

Les tests et les résultats sont documentés et analysés. Ils donnent lieu, si nécessaire, à une adaptation de la politique de continuité des activités et du BCP.

(b) modifications

Les modifications significatives que l'établissement apporte à son organisation, à sa prestation de services, à son programme d'activités et à son ICT, sont l'occasion d'examiner le caractère adéquat des dispositifs de continuité existants et du BCP et, si nécessaire, d'adapter ceux-ci en application des règles décrites ci-dessus.

Les entités et fonctions critiques concernées procèdent régulièrement à l'examen de leurs dispositifs de continuité et de leurs procédures détaillées afin de les adapter aux modifications affectant leur fonctionnement (personnel, moyens de communication, systèmes,…).

5. ***Implication des prestataires de services externes***

L'établissement qui, pour certaines sections relatives à la continuité de ses activités, fait appel à des prestataires de services externes, entreprend toutes les démarches raisonnables pour s'assurer que les services convenus seront disponibles en cas de nécessité, par exemple en veillant à une distance géographique suffisante entre les centres de secours et les centres opérationnels (voir annexe 1), ou en intégrant dans la convention de sous-traitance des garanties de capacité. En effet, si de nombreux établissements du secteur font appel au même prestataire de services, cela peut, en cas de désastre, mettre en péril la qualité et la disponibilité de ses services.

Pour cet aspect et d'autres points importants à prendre en considération en cas de sous-traitance, l'on se reportera également à la circulaire de la FSMA sur les saines pratiques de gestion en matière de sous-traitance disponible sur le site internet (http://www.fsma.be/fr/Supervision/finbem/bo/circmedprak/vvb.aspx).

⁂

Annexe 1

Critères pour la détermination de la distance minimale entre les centres ICT et les centres de secours

De façon à tenir compte de la diversité des profils de risque, il revient aux entreprises visées par la présente circulaire de procéder à leur propre évaluation des risques de façon à arrêter la distance minimale adéquate entre leurs centres ICT et de secours pour les systèmes ICT critiques. Dans cette dernière, il convient de tenir compte au minimum des éléments suivants :

- la destruction potentielle de *datacenters* et de centres opérationnels entiers, en ce compris la perte de personnes-clé ;
- les risques géologiques et météorologiques (inondations, tremblements de terre, etc.) ; une situation où l'ensemble des *datacenters* seraient localisés dans une même zone sujette à inondations ne pourrait être acceptée ;
- les risques environnementaux (proximité d'activités industrielles à profil de risque élevé, aéroports, ambassades, organisations gouvernementales et militaires, etc.); la distance entre *datacenters* devrait ainsi par exemple être plus élevée si l'un de ceux-ci se situe dans les environs immédiats d'une centrale nucléaire ou d'une cible potentielle d'attaques terroristes, tels que les sièges d'institutions internationales; de même, les *datacenters* qui sont localisés dans des grandes agglomérations et des zones à activité industrielle dangereuse devraient – dans le contexte de ce risque – observer des distances de sécurités plus grandes ;
- la possible inaccessibilité des *datacenters* et des locaux opérationnels du fait de perturbations sociales, évacuations, périmètres de sécurité, destruction ou congestion des voies d'accès; les situations dans lesquelles l'accès au centre de secours est dépendant de la possibilité d'utiliser des voies d'accès qui risquent d'être bloquées en cas d'incident au niveau du centre ICT primaire doivent être évitées ;
- les dégâts pouvant résulter d'attaques terroristes dirigées contre une infrastructure ou une institution financière critique ou son environnement ;
- les dégâts à l'environnement immédiat et aux fournitures de services d'utilité publique ; dans ce contexte, il est essentiel que les centres ICT et de secours utilisent des fournisseurs de services d'utilité publique qui ne présentent pas des "*single points of failure*" et qui sont géographiquement suffisamment éloignés les uns des autres pour ne pas être atteints par un même incident à caractère local ; dans des régions rurales où le maillage et la redondance en matière de services d'utilité publique sont moindres, la distance de sécurité minimale entre les *datacenters* devrait être plus grande que dans les agglomérations ou zones industrielles avec un maillage et une redondance élevés.

⁂