COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

PLANS ET SYSTEMES DE CONTINUITE D'ACTIVITE (BCP)

Résultats du recensement des BCP et considérations prudentielles

Table des matières

Liste des observations

1. L'OBJECTIF DU RECENSEMENT

L'objectif du recensement des «Business Continuity Plans» (BCP) sur base d'une lettre circulaire du 11 septembre 2002 était de permettre à la Commission de Surveillance du Secteur Financier (CSSF) d'avoir une vue d'ensemble sur les plans de continuité d'activité et sur leur application dans la pratique auprès des institutions financières et autres professionnels du secteur financier (PSF). L'objectif n'était pas de valider les choix de ces établissements.

Le premier intérêt prudentiel pour la CSSF réside dans l'analyse des méthodes de la gestion des risques potentiels telle qu'elle est assurée dans le cadre de plans de continuité, ceci dans l'intérêt de la pérennité des établissements en cas de sinistre et dans l'intérêt de l'intégrité des droits de leurs clients.

En effet, la poursuite de l'activité après un sinistre, informatique ou autre, est essentielle pour l'établissement touché qui risque de subir en cas de rupture non seulement des pertes financières occasionnées par le sinistre-même, mais également des pertes de revenus sur l'activité qui ne peut plus être assurée ainsi que les effets d'une publicité négative, voire une perte de confiance de la part de sa clientèle.

Au-delà de l'impact sur l'établissement, la non-continuité touche aussi les contreparties de celui-ci et le marché en général du fait de l'effet systémique. Ce risque systémique est réel et, en raison de la globalisation des échanges et des transactions financières, ne reste pas limité au seul secteur financier national.

Si un établissement financier venait à subir un sinistre lui imposant d'arrêter ses activités, il serait considéré de fait comme une contrepartie défaillante par les autres acteurs, ne garantissant plus l'aboutissement et la liquidation (settlement) de contrats sur produits financiers, paiements, contrats de change, crédits, garanties sur titres, prêts de titres, etc.. Cette défaillance sera, dans le meilleur des cas, financièrement pénalisée par l'application d'indemnités calculées sur base des taux de financement (taux d'intérêt) jusqu'au retour à une situation normale, mais dans le pire des cas, l'établissement défaillant se trouve en rupture de contrat, rupture qui déclenche les clauses «default» et «cross default».

Le recensement fait par la CSSF a eu un effet induit de sensibilisation sur un grand nombre d'établissements interrogés qui ont pris conscience de l'absence de BCP au sein de leur organisation. La prise de conscience du besoin d'un plan de continuité d'activités ou la remise en question des plans existants a augmenté à la suite du recensement.

2. LA STRUCTURE DU QUESTIONNAIRE

Le questionnaire adressé aux différentes institutions financières visées par le recensement a été établi de manière à pouvoir être exploité aussi bien par des établissements de petite taille que par de grandes banques faisant éventuellement partie de grands groupes internationaux.

Pour cette raison, le questionnaire a été divisé en deux parties. La première partie pose certaines questions d'ordre général quant à l'existence d'un BCP, sa date de première mise en place et sa date de dernière modification, les personnes à l'origine du plan et celles étant intervenues pour sa conception et sa réalisation ainsi que l'approche utilisée (approche par les causes ou les conséquences).

La nature des questions posées, notamment en ce qui concerne les personnes impliquées et/ou l'origine du plan, avait pour but de déterminer le niveau hiérarchique qui est intervenu dans l'élaboration de ce plan. Cette dernière information donne une indication non seulement sur

l'implication des organes de décision de l'établissement, mais également si ce plan a été élaboré par des «techniciens» de l'informatique ou à un niveau organisationnel plus élevé, tel que le département organisation ou la direction elle-même.

La question relative à l'approche utilisée permet d'obtenir une appréciation de la qualité du plan. En effet, l'approche orientée sur les conséquences, telle la destruction totale ou partielle des infrastructures (informations financières, indisponibilité de l'ordinateur central ou des serveurs délocalisés, etc.) ou leur indisponibilité temporaire, permet théoriquement de couvrir toutes les causes possibles (incendie, crash, tremblement de terre, attentat, etc.), l'inverse ne l'étant pas.

La seconde partie du questionnaire concerne les BCP en eux-mêmes par activité, métier ou «business line». Le but de cette partie était de déterminer, pour les établissements disposant d'un tel plan par activité, quelles sont les activités, essentielles et prioritaires, pour les différents acteurs. Certaines questions plus spécifiques visaient à connaître les intervenants qui recourent à des centres de back-up partagés, de manière à identifier un risque probable de concentration auprès d'un même prestataire et donc un éventuel risque systémique pour la place financière dans son ensemble, le prestataire ne pouvant secourir tous ses clients en même temps si un sinistre collectif affecte plusieurs organismes financiers ou, pire, s'il se trouve dans la même zone géographique que celle des sinistrés. Le risque est par ailleurs augmenté si plusieurs prestataires se trouvent concentrés dans une même zone géographique.

3. DÉFINITION D'UN BCP

Un BCP est un processus consistant à étudier et à développer à l'avance des dispositifs et des procédures permettant à une organisation de faire face à des événements invalidants, pouvant survenir par malchance ou par des circonstances imprévisibles, voire inconcevables, en adoptant des solutions de repli efficaces et applicables à toutes occasions d'une manière telle que les fonctions critiques de son activité puissent être continuées sans interruption notable ou changement radical ou essentiel.

Il s'agit donc d'un plan qui doit décrire avec précision :
- les étapes, procédures et tâches à réaliser lors de l'apparition d'un sinistre,
- la mise en place des solutions de secours/repli, afin de permettre la restauration de l'environnement et la poursuite de l'activité en régime «normal».

4. LES PRINCIPAUX RÉSULTATS DU RECENSEMENT

a. Remarque préliminaire

Cette partie a pour objectif de dresser un état des lieux de l'existence et de la pratique de BCP auprès des établissements de crédit et autres professionnels du secteur financier établis au Grand-Duché de Luxembourg et soumis à la surveillance prudentielle de la CSSF.

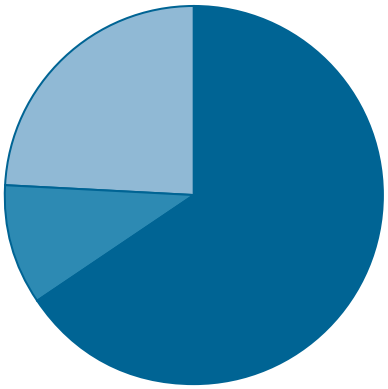
b. L'existence d'un BCP

Cette question visait en premier lieu à distinguer les établissements ne disposant pas d'un BCP au vrai sens du terme des établissements disposant d'un véritable BCP, à savoir avec des mesures concrètes et des procédures adéquates rendant l'institution financière réellement capable de poursuivre ses activités, particulièrement celles qui sont critiques, pratiquement sans interruption et à un niveau qualitatif acceptable.

Il faut souligner que la portée d'un BCP, dont il est question ici, est nettement plus vaste que la simple définition de back-up énoncée au point 4.5.2.1. de la circulaire IML 96/126. Le BCP ne devrait en effet pas être compris comme simple back-up informatique, c'est-à-dire comme sauvegarde de données informatisées (en général, des fichiers sur supports magnétiques permettant de reconstruire une situation antérieure aux dernières vingt-quatre heures).

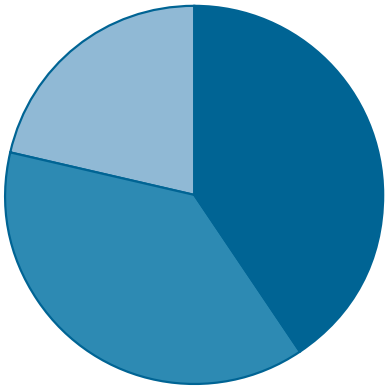
Comme le montrent les graphiques ci-après, surtout si l'on considère la part des «oui», la situation au niveau des PSF nécessite une prise de conscience significative. Au niveau des banques, les institutions n'ayant pas de BCP à proprement parler disposent néanmoins d'un back-up tel que requis par le point 4.5.2.1. de la circulaire IML 96/126. A noter également que la direction ou les responsables de bon nombre d'institutions financières ont déclaré vouloir considérer la nécessité de l'élaboration d'un BCP dans un avenir proche sans pour autant avoir renseigné un projet en cours. On peut donc espérer que dans le court et moyen terme la situation évoluera et que la place se dirigera vers une couverture plus généralisée des risques d'interruption des activités, et donc vers une meilleure protection contre le risque opérationnel.

Existence BCP BANQUES



Oui	65,66 %
Non	10,24 %
Projet en cours	24,10 %

Existence BCP PSF



Oui	40,94 %
Non	37,80 %
Projet en cours	21,26 %

Observation 1: Existence d'un BCP

La circulaire IML 96/126 prévoit dans son point 4.5.2.1. que les établissements doivent disposer d'un back-up informatique, qui s'apparente à un DRP (Disaster Recovery Plan). Il est actuellement opportun de faire évoluer ce DRP vers un BCP plus complet, qui englobe aussi bien l'outil informatique que les tâches critiques et les ressources humaines, étant donné que la circulaire 96/126 stipule en même temps que : «Par ailleurs, l'établissement doit être en mesure de fonctionner normalement en cas de panne de son système informatique et il élaborera à cet effet une solution de back-up[1].»

Par l'expression «fonctionner normalement», il faut entendre que l'établissement victime d'un sinistre ne devrait ni subir de diminution dans la qualité de services en-dessous d'un niveau prédéfini, ni subir d'augmentation des risques.

La notion de «panne informatique» doit être étendue à celle de «sinistre» qui couvre tous les besoins vitaux de l'établissement (locaux : salle machine, salle des marchés, bureaux, salles de réunions, guichets, …, télécommunications : lignes louées, lignes téléphoniques, …, systèmes informatiques).

[1] Il n'est pas absolument obligatoire d'avoir un back-up informatique complet. Voir à ce sujet également le point 5.c «L'existence et la forme de redondance».

c. L'influence des événements du 11 septembre 2001

La seconde question visait à obtenir une réaction quant à l'impact qu'ont eu les attentats terroristes de septembre 2001 sur les BCP existants et sur les considérations quant à l'opportunité de développer un tel plan. Seule une minorité (d'environ 20%) des établissements répond que les événements de septembre 2001 ont eu une influence sur les mesures et les procédures mises en place ou à prévoir. Essentiellement, cette influence se manifeste par une prise de conscience accrue de l'importance de disposer de mesures adéquates plus performantes pour minimiser les conséquences d'un désastre, par une accélération dans la réalisation des projets de BCP en cours ainsi que, marginalement, par une révision des objectifs des plans existants.

Les causes de sinistre doivent être vues de manière différente et complétées. Aux causes envisagées avant 11 septembre 2001 (incendie et dégâts des eaux, intempéries (inondations, foudre), erreur humaine, malversation (virus, piratage, …), etc.), il faut ajouter désormais celle du terrorisme massif portant sur la destruction de l'infrastructure (bombe, chute d'avion, etc.) et des prestataires tiers ainsi que l'indisponibilité du personnel qui peut en découler.

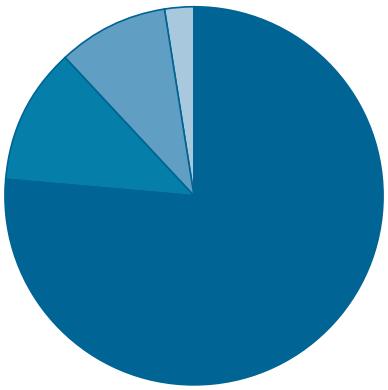
d. Le niveau hiérarchique initiateur du plan

Le but de cette question était de pouvoir fonder un jugement quant à l'implication d'un niveau hiérarchique suffisant, ainsi que de porter un œil critique et objectif sur les domaines couverts par le BCP. En effet, par expérience, on peut admettre qu'un BCP initié par le département ou le responsable informatique portera principalement sur la sauvegarde des données informatiques et la continuité acceptable de l'exploitation informatique. Ce type de plan ne tombe pas sous la définition d'un BCP réel et global et, comme déjà mentionné précédemment, il s'apparente à un DRP limité aux activités de l'informatique.

Par contre, on peut considérer qu'avec un plan initié par un niveau hiérarchique supérieur, tel que le conseil d'administration ou la direction, ou par une fonction indépendante, le département organisation, un établissement pourra avoir le recul, la vue d'ensemble et la qualité professionnelle nécessaire afin de couvrir la globalité des domaines de l'activité nécessitant d'être inclus. Parmi les établissements ayant renseigné l'existence d'un BCP, les données relatives à l'implication du niveau hiérarchique ayant initié le BCP sont reprises dans le graphique suivant.

Implication hiérarchique

Direction / Organisation	76,40 %
Maison-mère	11,80 %
Informatique	9,32 %
Pas de réponse	2,48 %



Observation 2: Implication hiérarchique

La bonne pratique suggère que le BCP soit initié par un niveau hiérarchique élevé. Ainsi, la prise de décision quant aux domaines à couvrir par le plan, sa méthodologie, etc., sont du ressort de la direction, impliquant en outre le conseil d'administration.

e. L'approche retenue

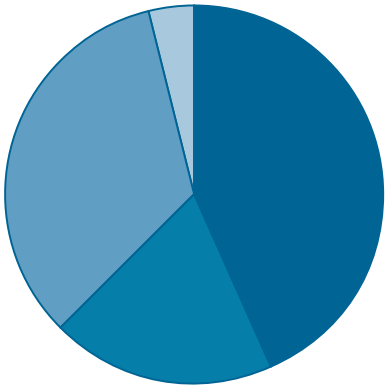
Cette question visait à faire la distinction entre les établissements disposant d'un BCP conçu sur base des causes probables de sinistre et ceux qui s'appuient sur les conséquences. Cette question permet à nouveau d'apprécier à certains égards la qualité du BCP, dans le sens où une approche basée sur les conséquences engendre généralement une analyse plus complète, plus fine et plus approfondie des moyens à mettre en œuvre pour assurer la continuité des activités. Une approche basée sur les causes risque de faire l'impasse sur certains scénarios, comme les attentats terroristes, et toutes les conséquences ne peuvent être que difficilement déterminées ex ante.

Certains organismes financiers ont renseigné les deux approches, ce qui peut être interprété de deux manières : soit la question n'a pas bien été comprise, soit ces établissements ont effectivement utilisé les deux approches afin de s'assurer de la globalité et de l'exhaustivité de leur analyse. Ne pouvant pas spéculer sur le niveau de compréhension de cette question, on peut néanmoins partir de l'hypothèse que les établissements adoptant les deux approches l'ont fait dans le but d'assurer l'exhaustivité de la couverture du problème.

Parmi les établissements ayant renseigné disposer d'un BCP, la répartition est reprise dans le graphique qui suit.

Approche utilisée

Conséquences	43,48 %
Causes	19,25 %
Les deux	33,54 %
Pas de réponse	3,73 %



Observation 3: L'approche utilisée

Même si on reconnaît à l'approche par les conséquences un avantage sur celle par les causes, on ne peut pas attribuer a priori une préférence à une approche ou une autre. Une méthodologie, quelle qu'elle soit, doit être adéquatement adoptée, appliquée et documentée.

Evaluer le type de sinistre (causes) et en déduire ensuite les plans de continuité a comme inconvénient que tous les sinistres ne peuvent être prévus, mais comme avantage que chaque sinistre est parfaitement maîtrisé.

Ne pas se préoccuper du sinistre et envisager une reprise complète par métier (conséquences) a comme inconvénient l'absence de finesse dans l'analyse et comme avantage de faire face à tous les cas qui se présenteraient. Une telle démarche peut également s'avérer plus coûteuse à mettre en œuvre.

Il n'appartient pas à l'autorité de contrôle de définir une méthodologie d'analyse et de mise en œuvre d'une solution de secours unique, mais il se recommande de suivre la démarche ci-après :

- Evaluer les risques de sinistres par rapport aux bâtiments (nature et localisation physique), à l'environnement de la salle machine, à la proximité immédiate de sites à risque (industriels ou autres). Il se peut, par exemple, que les risques d'infiltrations d'eaux soient plus importants que ceux d'incendie, ou que les risques d'attentat priment sur les autres à un moment donné.
- Pour chacun des sinistres retenus, analyser l'impact sur l'activité, c'est-à-dire pour chaque activité, déterminer les conséquences du sinistre sur le fonctionnement normal. Ces conséquences ne peuvent être estimées qu'en comparaison avec la qualité habituelle, ce qui veut dire que cette qualité est censée être définie et formalisée.
- Pour chaque activité, définir une solution théorique de secours qui minimise l'impact du sinistre sur la qualité. Il peut s'avérer nécessaire de définir un seuil minimal de tolérance en-dessous duquel la dégradation est inacceptable.
- Evaluer au mieux les coûts de chaque solution théorique de back-up.
- Explorer les combinaisons de solutions de back-up de manière à optimiser les ressources nécessaires à la mise en œuvre.
- Retenir les combinaisons les plus performantes, c'est-à-dire celles dont les coûts sont les plus faibles pour une dégradation minimale, voire nulle.
- Mettre en œuvre les solutions retenues et développer le plan de contingence, c'est-à-dire décrire les modalités, tâches et travaux à réaliser à l'apparition du sinistre, pendant l'utilisation de la solution de back-up et après la réparation du sinistre, lors du retour à la situation antérieure.

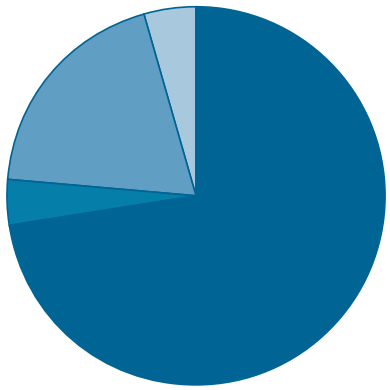
Cette démarche doit permettre de mettre l'accent sur l'analyse de tous les facteurs importants pour la poursuite des activités, c'est-à-dire pas uniquement l'informatique et les télécommunications, mais également les locaux et la mobilité du personnel.

f. L'analyse des risques

La question avait pour but de déterminer si l'analyse des risques a été conduite selon une approche quantitative (c'est-à-dire chiffrée en termes de coûts pour l'entreprise) ou bien qualitative (temps de réponse, impact sur l'image de marque ou vis-à-vis de la clientèle) ou une combinaison des deux. La répartition est reprise dans le graphique suivant.

Analyse des risques

Qualitative	72,67 %
Quantitative	3,73 %
Les deux	19,25 %
Pas de réponse	4,35 %



On peut relever qu'une grande majorité des entreprises se basent sur une analyse qualitative des risques, ce qui offre l'avantage d'être plus simple et moins onéreux au niveau de l'élaboration de l'analyse. Les établissements se basant sur une analyse quantitative sont marginaux et d'une taille relativement faible en termes d'employés (moins de 50 personnes). Les établissements combinant les deux approches sont généralement d'une taille relativement importante.

Observation 4: L'analyse des risques

Dans ce domaine également, il n'existe pas de choix préféré entre une approche qualitative et une approche quantitative, mais la détermination et l'analyse des risques principaux auxquels un établissement est confronté doivent être effectuées selon une méthodologie préalablement définie et documentée. Il faut cependant noter qu'une approche quantitative apparaît souhaitable pour les établissements qui devront appliquer le Nouvel Accord de Bâle (Bâle II), afin de mesurer la part du risque de sinistralité au sein des risques opérationnels.

Dans le but de déterminer les activités qui nécessitent un back-up informatique, il faut définir et étudier la fonction d'indisponibilité informatique f_a (durée, montant des pertes) [pour toute activité; a est une activité spécifique]. La difficulté vient à partir du moment où il existe une relation entre fonctions, ce qui est en général le cas, de sorte que la fonction à étudier devient f_a (durée, montant des pertes, $f_{a'}$, $f_{a''}$).

Etant donné qu'il n'est pas aisé de déterminer une fonction d'une telle complexité, l'usage d'une méthodologie peut être d'une aide précieuse.

Pour information, il existe de multiples travaux méthodologiques dans ce domaine et à titre d'exemple, en voici six qui sont relativement connus.

La méthode **MARION** (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) de notation des risques, qui a servi à l'élaboration de la méthode **Méhari** (MÉthode Harmonisée d'Analyse de RIsques), **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) qui est une méthode d'appréciation et de traitement des risques relatifs à la sécurité des systèmes d'information, la méthode **Octave** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) ou encore les travaux du NIST (National Institute of Standards and Technology) qui a écrit l'un des documents de référence dans le domaine, à savoir le «**Risk Management Guide for Information Technology Systems**». La norme **ISO 13335-2** est également très prometteuse, bien qu'étant encore en phase de développement (collecte de commentaires), mais sur le point d'être publiée.

Quelle que soit la méthode, il convient de préciser qu'il ne faut pas perdre de vue les enjeux d'une analyse des risques. Il convient par conséquent de ne pas négliger la notion de «valeur» des éléments sujets à analyse de risque. Ainsi, une activité qui utilise des ressources critiques devrait au préalable subir un processus d'évaluation financière, de manière à déterminer l'opportunité d'une analyse de risques plus approfondie. La quantification de la criticité des éléments ou de l'activité permet éventuellement d'optimiser la phase d'analyse de risques, en se concentrant sur ceux les plus critiques en terme de valeur.

L'analyse des risques se fera par conséquent également sous un angle financier, en prenant en compte :

- les contreparties du secteur
  - Le risque systémique intervient dès que l'établissement n'est plus présent vis-à-vis de ses contreparties (-> opérations d'arbitrage).
- les clients institutionnels
  - Intérêts courus sur les montants en dépôt, mais inaccessibles (-> déséquilibre entre les

engagements à court et long terme).
  - Absence de contrôle des risques crédits.
- les clients privés
  - Rétention de la clientèle.

g. La ventilation des activités et les critères de ventilation

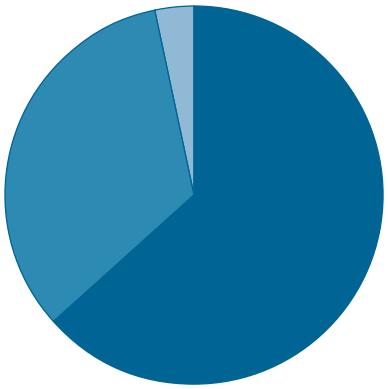
Cette question visait à donner une indication si les activités reprises dans le BCP sont ventilées selon des critères donnés, tels le niveau critique de l'activité, la fréquence ou le besoin en aval.

Au niveau des résultats, on constate bien évidemment que les établissements importants ayant plusieurs types d'activités ou faisant partie d'un groupe international, ont opté pour une ventilation des activités. Cependant, on constate également qu'une très large majorité des institutions financières, toutes tailles confondues, procède à une telle ventilation.

Parmi les établissements disposant d'un BCP, la répartition est reprise dans le graphique suivant.

Ventilation des activités

Oui	63,35 %
Non	33,54 %
Pas de réponse	3,11 %



En ce qui concerne les critères de ventilation des activités les plus utilisés, on peut citer en premier lieu les fonctions critiques, telle l'exploitation informatique, par opposition aux fonctions de support. Pour la définition des fonctions critiques, la plupart des établissements définissent des intervalles de temps d'indisponibilité «tolérables». Ainsi, par exemple, les fonctions devant impérativement être restaurées dans les trois ou quatre heures sont considérées comme critiques, celles devant être restaurées dans un délai d'environ vingt-quatre heures sont définies comme essentielles, celles devant être restaurées endéans les quarante-huit heures comme nécessaires. Les autres critères renseignés sont le besoin en aval, suivi de l'impact financier, de l'impact légal ou de l'effet sur la clientèle.

Observation 5: Ventilation des activités

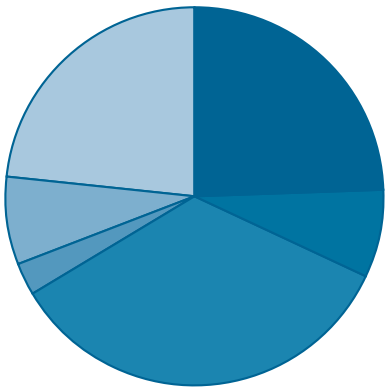
Une bonne pratique consiste à établir une liste fixant les priorités des activités selon des critères précis, préalablement établis.

h. L'existence et la composition d'une cellule de crise

Le but de cette question était d'obtenir une indication de l'implication de la direction des établissements dans la cellule (ou le comité) de crise lors de l'activation du plan, ainsi que de cerner les connaissances et les compétences les plus fréquemment rencontrées dans de tels comités ou de telles cellules. Ainsi, parmi les organismes financiers ayant déclaré avoir un BCP, 89% ont également instauré une cellule (ou un comité) destinée à gérer des situations exceptionnelles de crise. Le graphique ci-après reprend les principales typologies au niveau de la composition de tels comités.

Composition de la cellule de crise

Direction	24,48 %
Direction + IT	7,69 %
Direction + IT + Fonctions de support (resp. service, orga)	34,27 %
Responsable BCP + Direction	2,80 %
Responsable BCP + Direction + Fonctions de support (IT, orga, audit)	7,69 %
Autre / Pas de détail	23,08 %



Il est à noter que dans pratiquement tous les cas où une cellule de crise existe, la direction y est représentée. Ceci est un indicateur du niveau de prise de conscience du problème et de l'importance qui lui est attribuée.

Observation 6: Cellule de crise

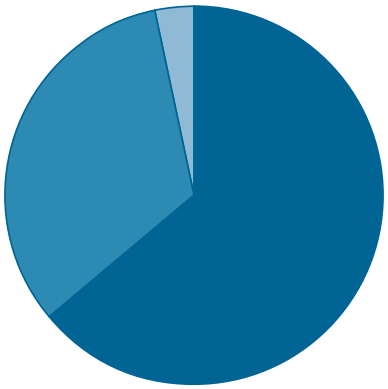
Au vue de l'importance que revêt la gestion adéquate d'une crise, la mise en place d'une cellule de crise impliquant la direction de l'établissement ainsi que la définition claire des rôles et responsabilités des membres d'une telle cellule est une constante parmi les établissements disposant d'un BCP. La composition, les rôles et les responsabilités des membres de cette cellule doivent être connus de l'ensemble du personnel. Pour chaque membre actif, il convient de désigner un suppléant. Il est primordial que la cellule de crise puisse communiquer et agir efficacement à l'égard les différentes autorités publiques. Les autorités publiques (police, protection civile, CSSF, etc.) devraient par conséquent connaître l'identité et les coordonnées de la personne de contact au sein de la cellule de crise.

i. La définition de critères d'activation précis

La définition de critères d'activation précis, préalablement bien établis et bien répertoriés protègent contre des ambiguïtés au moment du déclenchement du plan. Ceci permet principalement d'éliminer une grande partie du facteur subjectif de la (ou des) personne(s) désignée(s) comme responsable(s) pour la décision d'activer ou non le BCP. En effet, il s'agit souvent là d'un moment où le niveau de tension psychologique peut être très élevé, où la direction peut être momentanément indisponible et où le processus de décision risque d'être perturbé. Parmi les institutions renseignant un BCP formalisé, on constate la répartition suivante au niveau de l'existence de procédures d'activation précises.

Définition de procédures d'activation

Procédure d'activation précise	63,98 %
Pas de procédure précise	32,92 %
Pas de réponse	3,11 %



Parmi les établissements ayant répondu qu'ils disposent d'une procédure d'activation précise, on relève que près de deux tiers ont indiqué avoir des critères précis et principalement basés sur l'inaccessibilité, voire la destruction totale ou partielle de l'infrastructure (bâtiments en particulier) ou une indisponibilité des systèmes informatiques.

Observation 7: Procédures d'activation

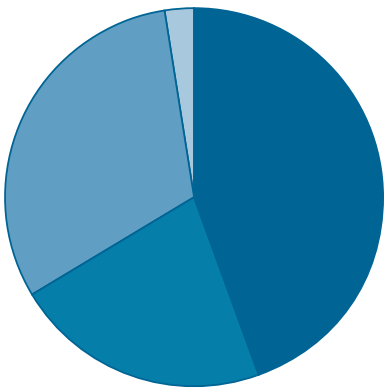
Au vu des réponses, il faut souligner l'importance d'une procédure de déclenchement du plan de secours et d'une procédure qui définit la façon de revenir à l'état normal de production. Les procédures d'activation et les critères y conduisant doivent être définis et connus au moins par les membres de la cellule de crise, et de préférence par l'ensemble du personnel. Cette procédure peut également permettre d'analyser les sources du sinistre afin de donner des indications utiles permettant d'améliorer la sécurité. L'établissement et la consignation de critères d'activation précis et sans ambiguïté sont d'usage afin de permettre d'activer le BCP à temps sans courir le risque des frais d'une activation inutile.

j. L'inclusion d'un plan de communication interne et externe dans le BCP

La confiance des clients, du public et des correspondants professionnels, ainsi qu'une communication adéquate et transparente sont deux éléments essentiels de l'activité bancaire et de la stabilité des marchés financiers. Cette confiance peut être ébranlée à l'apparition d'une crise alors qu'il y a absence d'un plan de communication efficace. Les résultats du recensement à ce sujet dégagent que plus de la moitié des établissements ayant un BCP formalisé n'y ont pas inclus un plan de communication interne et externe.

Existence d'un plan de communication

Plan interne et externe	44,72 %
Plan interne uniquement	21,74 %
Pas de plan de communication	31,06 %
Pas de réponse	2,48 %



Observation 8: Plan de communication

Il faut se rendre à l'évidence qu'en période de crise, il est difficile, voire impossible, de commencer à définir une communication efficace. La définition au préalable d'un plan de communication, aussi bien interne qu'externe, est essentielle et devrait faire partie intégrante de tout BCP. Les publications d'experts en matière de BCP soulignent que les personnes responsables de la communication externe doivent être nommées ; leur identité et coordonnées doivent être transmises aux autorités. A titre d'exemple, des listes de contacts internes et externes, des communiqués de presse ainsi que des lettres «type» à la clientèle peuvent aider la tâche des personnes en charge de la communication.

k. La protection des sites Internet

Pour des raisons similaires à celles évoquées au point précédent, la protection des sites Internet et de l'image qu'ils véhiculent est également importante, d'autant plus que des personnes mal intentionnées peuvent saisir l'opportunité d'une situation de crise pour s'attaquer à un site dans le but de le défigurer ou le détourner. Parmi les institutions financières déclarant disposer d'un site Internet, toutes catégories confondues (informatif, consultatif ou transactionnel), toutes déclarent disposer des moyens techniques de protection adéquats (firewall) et/ou d'une redondance des équipements informatiques, sans mentionner explicitement que la protection des sites, ou de l'image qu'ils véhiculent, fasse partie réellement du BCP global de l'établissement.

Observation 9: Protection des sites Internet

Il est indiqué que la protection des sites Internet, en fonction de l'appréciation de l'importance que représente cette activité pour l'établissement, fasse partie du BCP afin d'assurer leur pérennité. Le site Internet peut également être utilisé comme support de communication en période de crise.

l. La prise en compte de menaces intentionnelles (cyber-terrorisme, sabotage)

Cette question, faisant suite à celle concernant la protection des sites Internet, a été interprétée par la plupart des institutions financières comme question en relation directe avec leur site Internet. Elles n'ont pas abordé cette question de façon globale en prenant en considération leur protection face à des menaces intentionnelles. Cependant, en considérant la question quant à l'approche utilisée (causes et/ou conséquences), on peut supposer que les institutions basant leur approche sur les conséquences ou sur les causes et conséquences (soit près de 80%) couvrent d'office ces menaces.

Observation 10: Prise en compte de menaces intentionnelles

Les BCP se basant sur les conséquences englobent, en principe, la couverture du risque de telles menaces. Pour les BCP se basant sur les causes et suite aux événements du 11 septembre 2001, il est dorénavant raisonnable de prendre également en considération les menaces intentionnelles comme le terrorisme, le sabotage, la grève, les émeutes, etc., à côté des menaces plus classiques comme les incendies, dégâts des eaux ou pannes informatiques, de réseaux, d'électricité, de télécommunication.

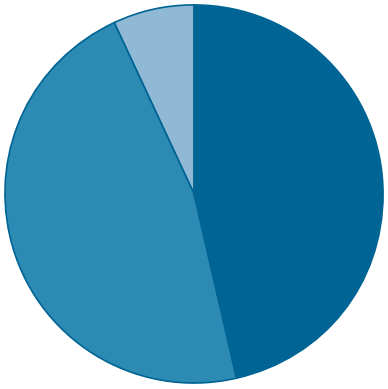
5. RECENSEMENT DES BCP PAR ACTIVITÉ

a. L'existence d'un BCP par activité

Parmi les établissements disposant d'un BCP formalisé, on constate qu'une très large majorité a ventilé les activités par priorité de rétablissement de celles-ci et a donc déterminé un niveau critique des activités. Les institutions financières qui ne renseignent pas de ventilation, se concentrent essentiellement sur la récupération de leurs outils de travail (principalement informatiques) et se limitent donc à la remise en marche de l'exploitation (informatique). La répartition des BCP concernés est reprise dans le graphique qui suit.

BCP par activité

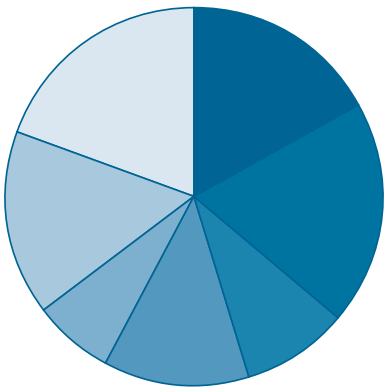
Oui	46,58 %
Non	46,58 %
Pas de réponse / détail	6,83 %



Parmi les institutions renseignant une ventilation des activités, quelque 55% répertorient les activités en question. On distingue très clairement ci-après l'activité principale des institutions en fonction de l'ordre des activités ou «business lines» énumérées.

Principales activités

Fonds	17,0 %
IT	19,3 %
Private Banking	9,1 %
Salle des marchés	12,5 %
Titres	6,8 %
Toutes les activités	15,9 %
Pas de détail	19,3 %



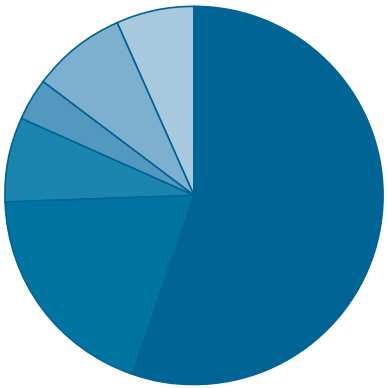
Ainsi, on retrouve les activités principales des institutions financières de la place, à savoir, par ordre décroissant, les fonctions de banque dépositaire de fonds d'investissement, l'activité sur les marchés interbancaires et l'activé dans le domaine du private banking.

b. La révision et le test des BCP

Une vaste majorité (85%) des institutions indiquent revoir régulièrement leur BCP afin de refléter et prendre en considération les changements intervenus, tant au niveau de l'organisation que des systèmes informatiques. En ce qui concerne la fréquence de cette révision, on constate sur le graphique ci-après que bon nombre d'établissements font une mise à jour annuelle de leur plan et des procédures.

Fréquence de revue

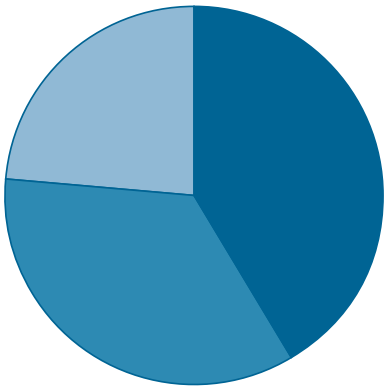
Annuelle	55,47 %
Semestrielle	18,98 %
Trimestrielle	7,30 %
Mensuelle	3,65 %
Autre / à la demande	8,03 %
Pas de réponse	6,57 %



Trois quarts des institutions financières procèdent à la mise à l'épreuve des plans à l'aide de tests. En matière de fréquence des tests et surtout du domaine couvert par ceux-ci, il y a lieu de bien distinguer les tests essentiellement informatiques de ceux impliquant aussi bien l'organisation interne que l'exploitation informatique et donc les départements opérationnels. Les résultats se synthétisent de la façon suivante.

Contenu des tests

IT	41,61 %
IT et organisationnel	34,78 %
Pas de réponse	23,60 %



Observation 11: Révision et test des BCP

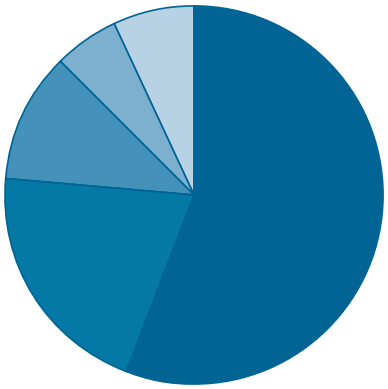
Les experts en la matière insistent sur l'importance des tests réguliers de plans de continuité. L'expérience montre également qu'un premier test d'un BCP n'est que rarement concluant. Il est primordial que les résultats de tests répétés et réguliers soient pris en compte afin d'améliorer la qualité du BCP et de valider sa pertinence. Un test annuel, prévoyant le cas échéant une rotation dans le choix des activités sélectionnées, constitue un minimum. En cas de rotation, la cohérence dans la couverture des différentes activités doit être assurée.

c. L'existence et la forme de redondance

Les institutions indiquent, pour la quasi-totalité (95%), disposer d'une redondance de leur traitement informatique sous une forme ou une autre. Un tiers des établissements indique même que certains traitements, principalement administratifs, peuvent être encore effectués manuellement ou en mode dégradé. En ce qui concerne le type de redondance (non manuelle) mis en place, le graphique ci-après indique très clairement que les organisations financières ont massivement recours aux services de prestataires externes.

Typologie de redondance

Prestataire	55,90 %
Entité du groupe au Luxembourg	20,50 %
Entité du groupe en dehors du Luxembourg	11,18 %
Même bâtiment	5,59 %
Pas de réponse	6,83 %



Le fait que la plupart des établissements disposent également d'une certaine duplication de leurs traitements informatiques dans leur propre bâtiment (machines de back-up, environnement de test, back-up des données, etc.), en plus d'un recours aux prestations d'un tiers, n'a pas été considéré comme redondance.

En effet, en cas de sinistre important au niveau du bâtiment, la redondance interne sera très probablement touchée et donc inutilisable. Ainsi donc, les institutions ayant déclaré avoir, en plus de leur solution interne, un recours ultime à un prestataire externe pour leur site de repli, ont été prises en considération sous la rubrique «prestataire externe».

Un phénomène similaire s'observe au niveau des succursales, qui ont parfois renseigné pouvoir être assistées par leur siège ainsi qu'avoir conclu des contrats de service avec un prestataire.

Dans ces conditions, et pour clarifier les situations et la classification, les établissements ayant répondu n'avoir recours qu'à une solution de redondance de traitement à l'intérieur du même bâtiment, respectivement n'avoir recours qu'à une entité du groupe en dehors du Luxembourg, ont été classés dans ces différentes catégories respectives. Les institutions, renseignant pouvoir se reposer sur une entité du groupe située au Luxembourg, disposent soit de leur propre site de repli, soit d'un second bâtiment vers lequel elles peuvent se replier et ont fait l'objet d'un classement sous la rubrique «entité du groupe au Luxembourg».

i. La problématique des centres de secours partagés

La circulaire IML 96/126 prévoit qu'en «*règle générale, l'établissement disposera dans des locaux à sa disposition au Luxembourg de ses propres ordinateurs …*». En théorie, il faut une salle blanche par établissement, mais la CSSF adopte une interprétation spécifique aux centres partagés et peut accepter une salle blanche multi-rack, hébergeant un ou plusieurs racks par établissement, à condition que chaque rack soit sécurisé et accessible uniquement à l'établissement. Le rack constitue alors le local minimum à usage exclusif de l'établissement.

Est considéré comme «centre partagé» une infrastructure permettant l'accueil des équipements provenant de plusieurs établissements pouvant cohabiter[2]. Les principales caractéristiques sont :
- une ou plusieurs salles équipées (détecteurs et extincteurs d'incendie, détecteurs eau et intrusion, alimentation de secours, …),
- des locaux aux accès contrôlés (y compris les salles blanches),
- une gestion commune ou syndiquée de l'infrastructure (y compris les réseaux locaux).

Les autres éléments fondamentaux de la circulaire IML 96/126 portent sur la confidentialité des données. La circulaire indique précisément au point 4.5.2. que «*les établissements doivent organiser leur fonction informatique de manière à en avoir le contrôle et à assurer sa qualité et de manière à garantir strictement la protection des données confidentielles qui leur sont confiées par leurs clients.*»

Cette responsabilité des établissements relative à la confidentialité des données est spécifiquement définie dans le cadre de la sous-traitance informatique : «*… il importe que les établissements ayant recours aux services de tiers respectent les conditions suivantes …*»

«*e) Pour des raisons de protection et de confidentialité les tiers en question ne peuvent pas avoir accès à des documents qui contiennent des données confidentielles.*»

«*f) L'interdiction d'accéder à des données confidentielles vaut également pour des tiers qui sont en charge de la gestion du système informatique. Si, dans le cadre d'une panne importante du système qui rend nécessaire un dépannage sur place, l'accès à ces données ne peut pas être évité, l'établissement doit veiller que le tiers en charge du dépannage soit accompagné tout au long de sa mission par une personne de l'établissement en charge de l'informatique.*»

Lorsqu'un établissement fait appel à un centre de secours partagé, il se trouve en présence d'un tiers auquel il sous-traite certains services informatiques de back-up.

Dans le cas où le gestionnaire du centre de back-up, au moment du sinistre, abandonne physiquement ses locaux et loue temporairement ceux-ci à l'usage exclusif de l'établissement pour la durée de son sinistre, on ne se trouve pas en présence d'un tiers sous-traitant.

C'est d'ailleurs ce système qui est couramment utilisé par les établissements qui mettent en place des environnements de secours immédiatement opérationnels. Ils délocalisent leurs ordinateurs contenant la situation «miroir» de leur système de production. Les données présentes sur l'ordinateur de secours sont une copie conforme des données de production, avec un décalage éventuel de quelques minutes au plus.

La seule façon pour ces établissements de rester conforme à la circulaire IML 96/126 consiste à louer un espace exclusif auprès du prestataire du centre de secours ou d'un autre tiers, de manière à y placer les ordinateurs de secours qui ne sont plus accessibles que par l'établissement financier. La solution n'est conforme au cadre réglementaire que si les ordinateurs sont physiquement et logiquement protégés et contrôlés exclusivement par l'établissement financier. Il ne peut pas y avoir de connexion de ces machines à un réseau local ou distant qui les rendrait accessibles à des tiers.

[2] Notons que c'est la cohabitation qui requiert le plus d'attention au niveau réglementaire.

Si le centre est partagé, cela signifie qu'au moment où un sinistre contraint un établissement de faire appel au centre de secours, il se retrouve locataire d'une partie des locaux alors qu'une autre partie des locaux peut être occupée par d'autres établissements qui, soit sont occupés à tester leurs solutions de secours, soit sont dans le cas analogue d'un autre sinistre. Cette situation ne présenterait pas de problèmes si aucune des composantes des diverses solutions de back-up n'était partagée : chaque établissement présent sur le site serait alors utilisateur unique de l'infrastructure qui lui est assignée.

Or, ce n'est que rarement le cas, particulièrement pour trois ressources du centre partagé dont la mutualisation est fondamentale pour permettre une réduction des coûts en assurant une flexibilité maximale des diverses configurations requises par les adhérents : les équipements d'accès physique (badges), le central téléphonique et le réseau local.

Il existe par contre quatre inconvénients majeurs à cette solution, à savoir :
- la difficulté de vérifier la conformité et l'exhaustivité de la configuration,
- la confiance accordée à l'intégrité des logiciels de gestion des systèmes,
- le manque de transparence globale qui existe entre les différents établissements,
- le risque de perte de confidentialité.

ii. La difficulté de vérifier la conformité et l'exhaustivité de la configuration

La conformité et l'exhaustivité de la configuration se vérifient à l'aide d'un audit spécifique. Il s'agira de contrôler les fichiers de configuration et les procédures de chargement à suivre. Les procédures de chargement doivent inclure des tâches de vérification de l'intégrité des configurations chargées dans les systèmes. Il peut y avoir deux manières de pré-configurer l'attribution des ressources, mais cela dépendra également des équipements.

La première manière consiste, si les équipements le permettent, à configurer uniquement les ressources nécessaires à chaque établissement, sachant que pour chaque établissement qui vient partager les infrastructures, la configuration vient s'ajouter à la configuration initiale. Dans ce cas, il faudra veiller à ce que les ressources allouées en premier ne soient pas modifiées lors de l'installation sur site d'un nouveau locataire.

La seconde manière de configurer l'allocation des ressources consiste à envisager la combinaison des situations possibles, c'est-à-dire à prévoir autant de configurations qu'il y a de possibilités d'accueillir d'établissements différents sur le site.

Prenons l'exemple de quatre établissements adhérents au site de secours partagé et dénommés de A à D. La taille et les besoins des établissements peuvent différer, de sorte que les combinaisons d'accueil possibles sont limitées. Supposons les contraintes suivantes :
- A et B sont de taille importante et ne peuvent pas occuper le site au même moment,
- la place disponible après usage de A ou de B ne permet que la présence de C,
- C et D peuvent cohabiter, mais alors, ni A, ni B ne peuvent être accueillis.

Les configurations à prévoir seront donc : A, B, C, D, A-C, B-C, C-D. Il est alors possible de prévoir une réallocation différente des ressources entre le cas A et le cas A-C, en supposant que A cède de l'espace à C.

iii. L'intégrité des logiciels de gestion des systèmes

Les logiciels étant souvent «propriétaires» aux fournisseurs, les sources ne sont pas disponibles et il est difficile, voire impossible, de s'assurer de leur intégrité. Comme pour tout logiciel ou système d'exploitation de système informatique, après s'être enquis de la qualité du fournisseur et du produit (notoriété, certifications éventuelles, etc.), il faut supposer qu'une configuration correctement testée et inaltérable, reste pérenne. Si la configuration reste opérationnelle pour une période relativement longue, il est primordial de vérifier par certains tests choisis que la situation ne se dégrade pas.

Si une nouvelle configuration vient à être installée lorsqu'un nouvel établissement s'ajoute au partage des ressources, il est essentiel de dérouler à nouveau l'ensemble des tests pour s'assurer du cantonnement de chaque environnement.

iv. Le manque de transparence globale entre les établissements utilisateurs du centre partagé

En principe, chaque établissement va avoir une vue des éléments de configuration qui le concerne, et il n'y a que le fournisseur du centre de secours partagé qui peut avoir une vue complète.

Du point de vue légal, la loi ne permet pas à l'autorité de surveillance d'intervenir directement auprès d'un sous-traitant n'ayant pas le statut de banque ou de PSF. Par conséquent, la CSSF n'a pas le pouvoir de vérifier la fiabilité de la solution partagée dans son ensemble. La CSSF peut demander à chaque établissement financier qui utilise le centre partagé, de lui fournir un document concernant sa situation, mais chaque document analysé séparément ne donne pas encore l'assurance qu'il n'y ait pas de faille.

Une solution consisterait à ce que les établissements adhérents se groupent pour commanditer un audit indépendant des configurations. De cette façon, l'auditeur peut garantir la confidentialité des éléments qu'il analyse individuellement et il peut également se prononcer sur la fiabilité de la solution en terme d'isolement des participants.

Si le prestataire du centre de secours opte pour le statut de PSF «opérateur de systèmes informatiques et de réseaux de communication du secteur financier», tel que défini à l'article 29-3 de la loi du 5 avril 1993 relative au secteur financier, modifiée entre autres par la loi du 2 août 2003, il entre dans le champ de la surveillance opérée par la CSSF et il peut offrir des services supplémentaires d'administration des systèmes de secours, même si ceux-ci contiennent des données de production.

v. Le risque de perte de confidentialité

Si certains éléments du centre de secours sont partagés, cela signifie également que le fournisseur du centre de secours est le principal garant de l'intégrité et du cantonnement des ressources requis par le cadre réglementaire. En effet, c'est lui qui va administrer les configurations multiples. Par contre, toutes les protections devront être prévues pour qu'il ne puisse pas accéder aux informations manipulées au sein de l'infrastructure mise à disposition, sauf s'il dispose d'un agrément d'opérateur de systèmes informatiques et de réseaux de communication du secteur financier. Sans ce statut, le partage des ressources peut être considéré comme un service de sous-traitance dont le prestataire a la gestion globale et il ne peut à aucun moment avoir accès aux données ou documents comportant des informations confidentielles. Etant donné qu'il est impossible de préjuger de la nature, confidentielle ou non, des informations qui transitent sur le réseau d'un établissement en production, le seul moyen pour garantir cette confidentialité consiste à interdire l'accès aux données au sous-traitant du centre de secours partagé.

Observation 12: Redondance

Le bon sens voudrait qu'il ne soit pas nécessairement obligatoire de prévoir systématiquement un back-up informatique complet. En effet, certains processus peuvent se traiter manuellement pour la durée du sinistre à condition que l'éventuel retard accumulé puisse être absorbé sans conséquences financières pour le client et de manière raisonnable pour l'établissement. Il est tout à fait envisageable que la solution de back-up utilisée à la suite d'une panne du système informatique ne fasse pas appel aux moyens informatiques habituels, à condition que l'activité ne subisse pas de dégradation de la qualité et qu'il n'y ait pas d'augmentation substantielle des risques opérationnels. Les autres moyens mis en œuvre dans la solution de secours peuvent s'appuyer par exemple sur une augmentation des ressources humaines ou sur l'utilisation d'outils bureautiques (tableurs). Sous certaines conditions, il est également possible de recourir à un centre de back-up partagé.

Observation 13: Centre de back-up partagé

Le rack correspond au local minimal à usage exclusif de l'établissement, au sens de la circulaire IML 96/126, sous réserve qu'il soit situé dans une salle blanche d'un centre de secours partagé et que les conditions suivantes soient respectées :

- le rack ne doit contenir que des équipements de l'établissement ;
- le rack doit être sécurisé (fermé à clé (badge ou serrure), sous alarme) ;
- le rack ne doit être accessible qu'au personnel de l'établissement et, éventuellement, aux services de garde et de secours en cas de sinistre, mais une trace inaltérable est nécessaire ;
- les lignes de communication doivent être sécurisées (l'équipement cryptographique doit se situer dans le rack) ;
- le réseau local doit être sécurisé et à usage exclusif (utilisation d'un VLAN ou segmentation physique par patch panel). Le rôle de l'exploitant du centre partagé est de gérer les configurations d'accueil (accès aux locaux, patch-panel et/ou les VLAN, équipements de sécurité des salles blanches) ainsi que de gérer la capacité d'accueil en évaluant correctement les risques de ses clients et son propre risque de concentration. Dans tous les cas de figure et plus particulièrement lors du recours de plusieurs clients au centre de secours, la confidentialité des données de chaque établissement doit être garantie.

d. Solution technique de redondance

i. Terminologie

Mirroring *(en français : disques en mode miroir)*[3]
Duplication des données d'un disque dur vers un second disque dur. En mode miroir, deux disques ou plus sont associés. Les blocs de données enregistrés sur le disque primaire le sont aussi sur le disque secondaire. Les disques fonctionnent en tandem ; ils enregistrent et mettent à jour les mêmes fichiers. En cas de défaillance de l'un des disques, l'autre continue de fonctionner, sans interruption ni perte de données.

Clustering
Groupe de plusieurs ordinateurs interconnectés et considérés comme une entité unique (machine virtuelle) pour diminuer le temps d'exécution d'une tâche en la fractionnant. En cas de défaillance de l'une des machines (couramment appelée *node*), sa charge de travail sera répartie automatiquement sur les autres systèmes sans pénaliser le logiciel et/ou l'utilisateur qui l'utilise.

Cold standby *(en français : salle blanche)*[4]
En matière de sécurité informatique, site équipé d'infrastructures et du matériel classique d'environnement, en excluant le matériel informatique (électricité, air conditionné, lignes de télécommunication, équipements d'administration), destiné à faciliter la reprise des activités de traitement après une catastrophe informatique. Cette configuration redondante est inactive et peut être mise en service manuellement en cas de défaillance du système principal et qui doit être complètement reconstruit.

Warm standby *(en français : salle redondante de secours manuel)*
Site équipé de matériel et de logiciels identiques à ceux du centre informatique à secourir, permettant ainsi, après restauration des données à partir d'une sauvegarde, de reprendre dans les meilleurs délais les activités normales de traitement.

[3] Dictionnaire de l'informatique: www.dicofr.com
[4] IBM : www.can.ibm.com/francais/dico/dictionnaire

Hot standby *(en français : salle redondante de secours automatique)*
Par l'utilisation de techniques de mirroring, site équipé de matériel, de logiciels et des données identiques (en temps réel) à ceux du centre informatique à secourir et pouvant être mis en service automatiquement, dans les meilleurs délais, en permettant de poursuivre les activités normales d'exploitation sans interruption.

ii. Les différentes approches de solution de redondance

Les différentes solutions techniques envisageables en matière de redondance, principalement les techniques de mirroring/clustering et la sauvegarde de données sur un support informatique (dans le but de permettre la restauration d'une situation antérieure), ont pour objectif de couvrir des risques sensiblement différents.

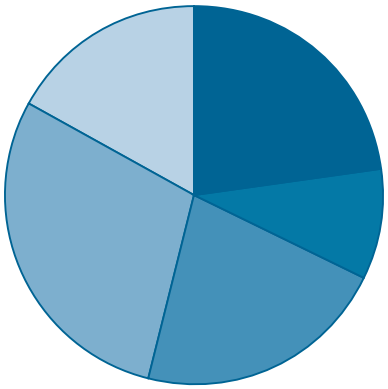
Ainsi, les techniques qu'on pourrait dénommer «temps réel», c'est-à-dire le clustering et le mirroring, ont principalement pour but de couvrir le risque d'interruption de l'exploitation informatique en assurant une disponibilité quasi immédiate en cas de défaillance du site de production informatique principal.

La technique qu'on pourrait appeler «back-up» ou «tape», outre de permettre la reconstruction de l'infrastructure logique après un désastre informatique, a pour objectif essentiel de se prémunir des risques opérationnels de saisie ou de programmation. Cette technique permet en effet de «revenir» à une situation antérieure considérée comme correcte ou exacte. A l'opposé, dans les techniques «temps réel», les erreurs de saisie ou de programmation sont automatiquement et directement répliquées sur l'environnement secondaire qui se trouve par là même tout autant corrompu. Par conséquent, une technique uniquement «temps réel» et non assortie d'une solution «tape» peut être extrêmement dangereuse et devrait donc être écartée. Un panachage des deux solutions semble raisonnable.

La répartition du type de redondance utilisée parmi les établissements disposant d'un BCP est la suivante.

Type de redondance

Clustering	22,98 %
Cold Standby	9,32 %
Hot Standby	21,74 %
Warm Standby	29,19 %
Pas de réponse / détail	16,77 %



Observation 14: Solution technique de redondance

Dans l'intérêt de l'établissement, celui-ci doit s'assurer d'avoir un plan de continuité qui lui permet de fonctionner en cas de sinistre et doit le distinguer d'une solution de back-up qui lui permet de restaurer des situations antérieures en cas de défaut de traitement (manipulation volontaire, par un virus, …). Dans tous les cas, l'établissement s'assurera qu'aucun tiers (maison-mère, prestataire) n'ait accès aux données confidentielles, sauf si le prestataire est un PSF répondant aux statuts décrits aux articles 29-1, 29-2 ou 29-3 de la loi modifiée du 5 avril 1993 relative au secteur financier. En ce qui concerne les centres de secours partagés, trois cas de figure peuvent se présenter.

1. L'équipement de secours contient les données de production (hot standby avec mirroring ou réplication) : l'établissement doit maintenir la confidentialité des données vis-à-vis des tiers (gestionnaire du centre de back-up et autres clients).

2. L'équipement est pré-configuré et prêt à accueillir des données de back-up : l'intégrité doit être assurée si l'équipement n'est pas sous contrôle avant usage.

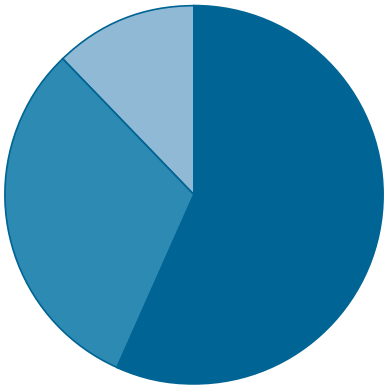
3. L'équipement est vide et prêt à recevoir toute une configuration de back-up : la fiabilité doit être validée si l'équipement n'est pas testé.

e. Le type de contrat avec le centre de back-up

Parmi les institutions financières faisant appel à un prestataire de service pour la mise à disposition d'un centre de back-up partagé, la répartition en fonction du type de contrat offert est la suivante.

Type de contrat

First in, First served	56,67 %
Prioritaire	31,11 %
Pas de réponse / détail	12,22 %



Le niveau de protection offert par ces deux types de contrat, en cas de sinistre sur une large étendue géographique, est très différent. Dans le type de contrat «first in, first served», le prestataire de service loue simultanément les mêmes postes de travail et équipements à plusieurs clients différents, qui peuvent éventuellement être situés dans une même zone géographique. En cas de sinistre touchant plusieurs clients, le premier sur place occupe les postes à disposition. Les autres peuvent se retrouver dans une situation où ils n'ont plus droit au service escompté. Ce type de contrat, qui est le moins onéreux, présente néanmoins un risque élevé en cas de sinistre touchant plusieurs établissements espérant avoir recours au même prestataire simultanément.

Dans le second type de contrat, dit «prioritaire», le prestataire partage en général une étendue géographique en plusieurs zones distinctes. A l'intérieur de chaque zone, il offre à un nombre limité de clients et éloignés géographiquement un accès prioritaire aux ressources. Les clients disposant d'un contrat «first in, first served» sont désavantagés et ne peuvent prétendre à

l'utilisation des postes lorsqu'un client «prioritaire» est dans une situation de sinistre et qu'il n'y a plus de postes disponibles. Ce type de contrat, nettement plus onéreux, bien qu'offrant une sûreté supplémentaire, ne garantit toutefois pas l'accès aux postes en cas de désastre touchant une très large étendue géographique ou une ville entière et donc un grand nombre de clients potentiels, comme ce fut le cas à la suite des événements du 11 septembre 2001.

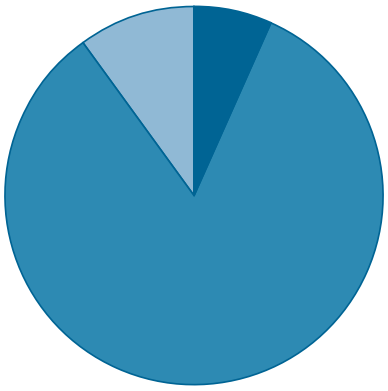
Au niveau de la place financière luxembourgeoise, le recours aux prestataires de centres de back-up est actuellement encore marqué par une concentration importante (voir point 5.c. «L'existence et la forme de redondance»).

f. La connaissance des autres clients du prestataire

Le genre de contrat que souscrivent les autres clients du prestataire et le type de protection auquel ces clients peuvent s'attendre, devraient théoriquement être pris en compte lors du choix d'un prestataire de centre de back-up. L'enquête dégage une situation négative en ce qui concerne l'information sur les autres clients d'un prestataire retenu, de leur contrat et de la proximité immédiate de l'établissement avec celui des autres clients.

Connaissance d'autres clients du prestataire

Oui	6,67 %
Non	83,33 %
Pas de réponse	10,00 %



Le détail des données fournies par ce recensement quant à la localisation de la production informatique et du site de repli ou de back-up, ne permet pas d'établir une cartographie détaillée et de détecter des risques éventuels de concentration auprès d'un même prestataire en fonction du type de contrat.

Il faut constater que les prestataires, qui ne sont pas soumis au contrôle prudentiel de la CSSF, jouent un rôle fondamental dans la stabilité du secteur financier au cas où un sinistre majeur viendrait à toucher une zone géographique à forte densité d'établissements financiers.

Observation 15: Clients des centres partagés

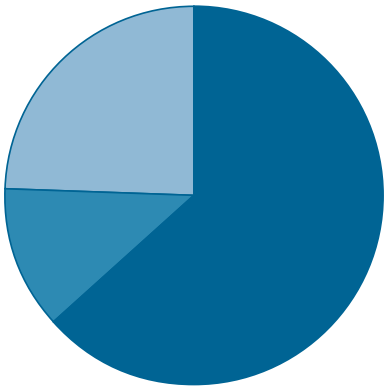
Les résultats de cette question suggèrent aux établissements ayant recours à un centre de back-up partagé d'obtenir les informations/la garantie sur la disponibilité des services achetés et le risque de concentration que subit le prestataire en fonction de sinistres parallèles et/ou touchant plusieurs de ses clients.

g. La gestion du risque de proximité par le prestataire

Près de deux tiers des organismes financiers, qui recourent aux services d'un prestataire externe pour la mise à disposition d'un site de secours, estiment que celui-ci gère le risque de proximité adéquatement, comme le montre le graphique ci-après.

Sentiment de gestion du risque de proximité par le prestataire

Oui	63,33 %
Non	12,22 %
Pas de réponse	24,44 %



Ces réponses sont à mettre en relation avec les résultats de la question précédente concernant la connaissance de l'existence d'autres clients chez le même prestataire et dans un voisinage proche. En effet, alors que plus de la moitié des établissements considèrent donc que leur prestataire prend en compte le paramètre de proximité dans le choix des clients auxquels il offre des solutions, plus de 8/10ième de ceux-ci ne connaissent ni l'existence des autres clients, ni leur type de contrat. Les clients de prestataires externes se sont donc montrés entièrement tributaires des informations que ces derniers leur transmettent et semblent ne pas avoir fait des analyses plus poussées à ce sujet.

Observation 16: Proximité par le prestataire

Un établissement devrait raisonnablement évaluer la distance entre le site de production et le site de secours de manière à éviter qu'un même sinistre puisse toucher les deux sites. La distance n'est cependant pas l'unique critère d'évaluation de la pertinence du plan de continuité. D'autres critères peuvent également être pris en considération (axes d'atterrissage et de décollage à proximité d'un aéroport, zone d'inondation, avenue ou boulevard important susceptible d'être bloqué lors de manifestations, …).

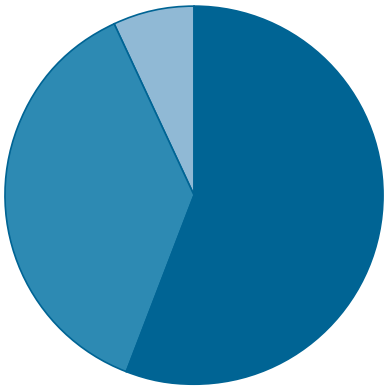
h. La ventilation incrémentale post-désastre des ressources et la prise en compte de potentielles pertes de ressources humaines

A la question «Votre BCP prévoit-il une ventilation incrémentale des ressources nécessaires entre l'incident et la reprise normale des activités?», une majorité d'établissements a répondu positivement, ce qui signifie que toutes les ressources ne sont pas censées être disponibles immédiatement, mais que le plan de continuité prévoit une montée en puissance de la reprise des activités en période de crise ou de désastre.

Cette situation s'explique principalement par la prise en considération du nombre limité de places au site de repli.

Ventilation des ressources

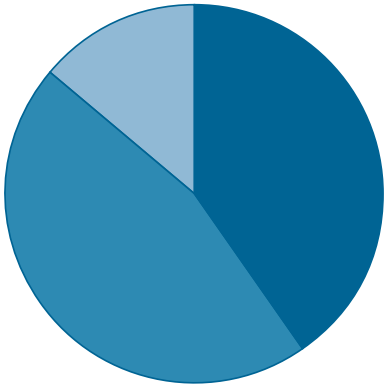
Oui	55,90 %
Non	37,27 %
Pas de réponse	6,83 %



La question relative à la prise en compte de possibles pertes de ressources humaines attire l'attention des responsables BCP sur la fragilité éventuelle de la planification optimale des ressources en cas de sinistre. Il est encourageant de constater que ce risque est pris en compte par 40% des institutions, comme le montre le graphique suivant.

Prise en compte de pertes des ressources humaines

Oui	40,37 %
Non	45,96 %
Pas de réponse	13,66 %



Observation 17: Pertes humaines

Les publications concernant les BCP, surtout suite aux événements du 11 septembre 2001, soulignent l'importance du facteur humain et montrent qu'il est essentiel de disposer d'une documentation et de procédures précises permettant à un département d'un établissement de continuer à fonctionner en cas d'indisponibilité de la majorité de son personnel. Cette documentation devra donc être formulée de façon à permettre une reprise plus rapide et plus efficace des activités par un personnel remplaçant ou intérimaire et devra être disponible, tout comme la documentation du plan de continuité, auprès du centre de repli.

i. La disponibilité, en externe, de toutes les données nécessaires au bon déroulement du plan (y compris les documents physiques)

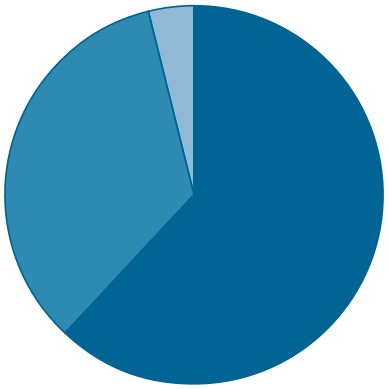
A la première partie de la question, à savoir la disponibilité en externe de toutes les données nécessaires au bon déroulement du BCP, les institutions financières semblent toutes avoir interprété dans le mot «données» la signification «données informatiques». En effet, elles ont, pour une très large majorité de 85,7%, déclaré disposer d'une copie des données sur supports informatiques auprès d'un prestataire externe.

Un phénomène similaire peut être observé à l'analyse des réponses concernant la prise en considération du besoin de documents physiques. En effet, il apparaît que bon nombre d'établissements ont compris par cette question la disponibilité du plan de continuité sur le site de secours. L'interprétation de cette question par la CSSF est nettement plus large puisqu'elle inclut tous les documents de l'entreprise, notamment la copie des différents contrats d'assurance, des clients et fournisseurs, la disponibilité des formulaires pré-imprimés, la copie des documents de procédures, etc..

En fonction des réponses données, une appréciation a été faite pour considérer si cette question avait été correctement comprise. Il n'est pas exclu que parmi la catégorie «oui» du graphique ci-après, se retrouvent des établissements qui considèrent uniquement la disponibilité du plan de continuité sur leur site de repli et non la disponibilité des autres documents de travail.

Disponibilité externe de documents physiques

Oui	62,11 %
Non	34,16 %
Pas de réponse	3,73 %



Observation 18: Stockage des données à l'extérieur

La pratique montre qu'en cas de sinistre, la redondance des infrastructures ne peut être efficace que si elle va de pair avec la disponibilité de l'ensemble des informations nécessaires à la continuité de l'activité.

j. L'évolution des investissements consacrés au BCP

Parmi les institutions financières ayant répondu à cette question, certaines ont fourni des chiffres en termes de pourcentage du montant global des investissements, d'autres du chiffre d'affaires, d'autres des frais généraux et d'autres encore du budget informatique.

L'unique élément exploitable des réponses fournies à cette question est l'évolution du chiffre consacré au BCP, quel qu'il soit, suite aux événements du 11 septembre. Uniquement 14 établissements sur 120 réponses fournies, soit un peu plus de 11%, déclarent avoir alloué davantage de moyens à leur BCP suite aux attentats du 11 septembre.

Observation 19: Coût/Budget d'un BCP

Il est dangereux de mettre en balance les coûts directs issus d'une solution BCP et les coûts directs d'une rupture. Ainsi, le raisonnement consistant à comparer le coût d'une solution de back-up aux coûts éventuels liés à la suspension d'une activité, est incomplet. Une comparaison de ce type ignore les risques de réputation qui peuvent engendrer une perte de confiance. Devant l'ampleur des montants à prévoir pour la mise en place de solutions de secours complètes pour faire face à un sinistre important, la tendance actuelle va vers la mutualisation des ressources et la sous-traitance.

Notons qu'il n'y a pas de lien direct entre les exigences en fonds propres du Nouvel Accord de Bâle (Bâle II) et le fait d'avoir un plan de continuité. Le BCP n'est pas un facteur qui permet de diminuer directement les besoins en fonds propres, mais une condition pour accéder aux différentes approches de l'Advanced Measurement Approach[5] (AMA) au niveau du calcul du risque opérationnel. Indirectement, un BCP performant devrait donc réduire les besoins en fonds propres étant donné qu'il permet de réduire le «estimated loss».

6. CONSIDÉRATIONS FINALES

Il ressort de l'analyse des réponses à l'enquête de la CSSF qu'un grand nombre de professionnels du secteur financier ont concentré par le passé leur attention essentiellement sur le développement de solutions de secours pour leur outil informatique. L'évolution, influencée non pas en dernier lieu par des événements comme ceux de septembre 2001, a toutefois fait évoluer les réflexions et un certain nombre de projets - vers une conception plus large des plans de continuité de l'activité. Une pareille approche holistique englobe l'ensemble des ressources nécessaires au fonctionnement, à savoir au moins le personnel, les locaux, les télécommunications, l'informatique et la documentation ainsi que les interactions entres ces divers éléments.

Il est théoriquement envisageable qu'un plan BCP au sens défini ci-avant soit réalisé au moyen de solutions se passant d'outils informatiques, pour peu que la qualité de la prestation de services reste raisonnablement assurée et surtout que la solution retenue n'augmente pas les risques. Néanmoins, dans la pratique, compte tenu de l'importance de l'informatique dans les activités des établissements financiers, il n'est quasiment plus envisageable de mettre en place des solutions de secours ne faisant pas appel à une redondance des systèmes informatiques.

L'utilisation des centres de secours partagés est une solution intéressante, surtout pour des établissements de plus petite taille. En adoptant une pareille solution, l'établissement doit toutefois veiller à respecter les contraintes d'une sous-traitance lorsqu'elle se situe en dehors d'un statut PSF au sens des articles 29-2 et 29-3 de la loi du 5 avril 1993 telle que modifiée entre autres par la loi du 2 août 2003, ces contraintes étant que :

- les systèmes et données de chaque établissement qui cohabite avec d'autres en utilisant des ressources partagées, doivent être parfaitement cantonnés par rapport à ceux des autres,
- le prestataire du centre de secours n'opère pas le système et n'est jamais en mesure de lire les informations confidentielles des établissements qui font appel à ses services.

La certitude sur la qualité et fiabilité des services prestés pourra être acquise à l'aide d'un audit complet qui couvre l'ensemble des éléments partagés et qui ne se limite donc pas à la somme d'analyses séparées faites par chaque établissement. Il s'agira d'étudier le centre de secours dans son ensemble. Des contrôles répétés devront garantir la pérennité des configurations retenues.

[5] qui sont : Internal Measurement Approaches, Scorecard Approaches, Loss distribution Approaches.

Indépendamment des solutions retenues par le BCP pour assurer une poursuite des activités en cas d'événements indésirables et perturbateurs, un établissement financier devrait s'assurer que les mesures mises en place sont réalistes, suffisantes et opérationnelles.

Ainsi, il serait judicieux que l'établissement procède régulièrement à un test complet de son BCP, en y incluant à la fois tous les éléments nécessaires à prouver la pertinence du test, c'est-à-dire au moins le personnel, l'infrastructure et les traitements, sans omettre l'aspect impromptu de l'événement. L'expérience tend à démontrer que les tests ne connaissent pas un déroulement similaire selon qu'ils ont été planifiés en informant les utilisateurs ou sans prévenir les utilisateurs concernés. Les activités de la salle des marchés, par exemple, peuvent se révéler extrêmement difficiles à poursuivre auprès d'un site de secours en cas d'interruption inopinée, en raison de la perte de contexte liée au changement d'infrastructure. Quels étaient les engagements à l'instant de l'interruption ? Si l'utilisateur est averti du test, il est probable qu'il anticipera cette situation délicate et s'arrangera pour avoir une situation stable à l'instant du test. Dans cet exemple, le test n'est manifestement pas complet étant donné que la situation initiale ne reflète pas celle de la réalité lors d'un événement inattendu.

Il convient, en conclusion de ce dossier, d'étendre les réflexions relatives aux BCP, en tentant d'analyser non seulement les facteurs d'échecs aux tests, mais également les situations qui ne se présenteront que lors d'une interruption inopinée en plein milieu de l'activité journalière, essentiellement si elle est du domaine de l'activité des marchés.

L'ensemble de cette analyse devrait permettre d'améliorer la vraisemblance des tests, en prenant cependant garde de ne pas compromettre la prestation des services à la clientèle, ce qui aurait une incidence directe sur la réputation en cas d'échec.

Il reste une question délicate à soulever, à savoir la fréquence à adopter pour de tels tests. Actuellement, la tendance indique une périodicité annuelle, mais sans préciser quel est le degré de complexité du test. La périodicité se décline en une équation complexe qui comprend à la fois les coûts et le risque d'échec.

La présente étude a pour premier objectif de fournir des informations factuelles sur la manière dont les professionnels du secteur financier luxembourgeois approchent la nécessité de disposer d'un plan de continuité de l'activité. Elle servira à sensibiliser les gestionnaires de ces professionnels à l'importance de revoir de façon critique la situation de leur entreprise au regard des impératifs d'une stratégie de pérennité, dans leur intérêt et dans celui de leurs clients et de la place en général.

Commission de Surveillance du Secteur Financier
110, route d'Arlon
L-2991 LUXEMBOURG
Tél. : (+352) 26 251-1
Fax : (+352) 26 251-601
E-mail : direction@cssf.lu
Internet : http://www.cssf.lu

Rédaction terminée le 1er mai 2004.

Conseil graphique : metaph