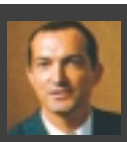
Gestion des risques

Les plans de continuité d'activité un élément important de Bâle II

Au centre des réflexions des régulateurs, *la question de la continuité des activités des banques est une préoccupation permanente du Comité de Bâle.*



ALAIN DEQUIER
Adjoint au directeur de la surveillance pour le système d'information Secrétariat général
Commission Bancaire

LA SITUATION ACTUELLE [1] PEUT se caractériser notamment par l'existence de plusieurs Livres blancs de la Commission bancaire qui incitent aux « meilleures pratiques ». Celui sur la sécurité des systèmes d'information de 1995-1996 conseillait de développer des secours informatiques et décrivait la disponibilité des données, des flux et des traitements. Ce premier facteur de sécurité de l'information parmi les quatre facteurs (à savoir la disponibilité, l'intégrité, la confidentialité, et la possibilité de preuve aussi nommée auditabilité ou traçabilité, ou DICP), est celui que les mesures de continuité renforcent.

UN CADRE RÉGLEMENTAIRE ÉVOLUTIF

Ce premier Livre blanc a inspiré la création d'outils de contrôle, pour les inspecteurs de la Commission bancaire, ou d'autocontrôle, pour la profession, qui permettent une évaluation du risque des systèmes d'information où la notion de continuité a un poids notable. Le Livre blanc sur le passage à l'an 2000, et surtout son addendum sur les plans de continuité [2], apportait des définitions précises (continuité, contournement, reprise, survie…) et une nouvelle approche, plus exigeante, par lignes de métiers, qui se retrouve aujourd'hui dans les travaux bâlois. Rappelons aussi qu'un règlement du Comité de la réglementation bancaire et financière, le CRBF 98/02, demandait de faire un rapport trimestriel aux organes délibérants sur l'état des secours mis en place pour le passage à l'an 2000. Les travaux ultérieurs, par exemple sur les conséquences prudentielles de l'internet, recommandent aussi la continuité de service. À la suite du passage à l'an 2000, les grands établissements ont maintenu des solutions de continuité mais le marché de ce type de service ne s'est pas réellement développé.

La continuité des activités relève de ce qu'on appelle les mesures de protection, celles dont l'objectif est de minimiser l'impact d'un événement défavorable, faisant le pendant aux mesures de prévention auxquelles correspondent souvent les mesures de contrôle interne, lesquelles tendent à réduire la probabilité de l'événement. Entre elles, peuvent s'intercaler des mesures de détection, qui visent à être informé très vite de l'événement pour réagir rapidement et ainsi en limiter les effets.

La situation purement réglementaire est toujours régie par le CRBF 97/02 et son article 14 pour les aspects traitement de l'information.

De nouvelles adaptations de ce règlement, déjà révisé en 2001 pour englober les entreprises d'investissement dans son périmètre, pourraient s'avérer utiles. En effet, depuis les événements tragiques de septembre 2001, la stricte notion de continuité, telle qu'elle était appréhendée, n'apparaît plus suffisante face aux scénarios qu'il faut à présent envisager. La robustesse ou résilience, c'est-à-dire la capacité de supporter des chocs extrêmes, doit à présent être l'objectif des mesures de protection.

ASSURER LA CONTINUITÉ DES ACTIVITÉS

La continuité est une préoccupation permanente des groupes de travail bâlois. Comme les réflexions françaises sur internet, les groupes qui travaillent sur le commerce électronique ou les services d'investissement estiment que la continuité est indispensable à ce type d'activité et que les éventuels modes de fonctionnement dégradés mis en place pour contourner une panne ou un incident ne doivent pas être perceptibles par la clientèle. Le groupe de travail sur les risques opérationnels qui a préparé un pan de l'accord Bâle II est explicite sur ce point : « *Banks* [3] *should have in place contingency and business continuity plans to en-*

« Depuis les événements de septembre 2001, la stricte notion de continuité, telle qu'elle était appréhendée, n'apparaît plus suffisante face aux scénarios qu'il faut à présent envisager. »

sure their ability to operate as going concerns and minimise losses in event of severe business disruption ». Ce constat conduit à s'interroger sur la manière dont l'existence d'un plan de continuité d'activité (PCA) pourra être prise en compte dans les différents piliers de l'Accord de Bâle.

Le pilier 1, sur l'allocation des fonds propres réglementaires, offre trois approches de calcul du risque opérationnel. Les deux premières calculent les fonds propres en proportion du produit bancaire global (approche basique) ou du produit bancaire différencié selon huit lignes de métier (approche standard), et n'ont donc pas de lien évident avec l'existence de plans de continuité dans l'établissement. Pour la troisième, ou plus précisément les suivantes – puisque, pour l'approche avancée, des variantes sont possibles –, une relation indirecte avec les PCA existe. En effet, les modèles de pertes que les établissements seront amenés à construire s'appuieront sur des statistiques internes d'incidents ou sur l'usage de bases de données d'incidents mises en commun. Comme c'est leur rôle, les PCA réduiront les effets des événements les plus graves qui auront justifié leur déclenchement. En cas d'usage de bases externes, il conviendra de retenir des cas semblables à ce qui peut se produire chez soi, donc ceux ayant bénéficié de l'effet modérateur d'un PCA. Si de tels cas ne sont pas disponibles, il faudra corriger les effets des scénarios extrêmes par l'apport modérateur du PCA mis en place dans l'établissement. De plus, dans les méthodes avancées il est envisagé de prendre en compte, dans une certaine limite, les assurances contractées. L'existence d'un PCA est un facteur favorable pour contracter une assurance et donc accéder à cet avantage sur le niveau de fonds propres.

Les exigences de Bâle II devraient sensiblement faire avancer les pratiques de contrôle et de suivi des risques opérationnels.

Un PCA réglementaire par type de métier

Le deuxième pilier de l'accord de Bâle fera jouer à plein l'existence d'un PCA. Ce pilier qui concerne les vérifications effectuées par le superviseur, devrait encourager l'usage d'outil informatisé d'appréciation de la sécurité informatique, comme c'est déjà pratiqué en France par les inspecteurs de la Commission bancaire. Ce genre de mesure sera étendu à l'existence d'un PCA réglementaire par ligne de métier. Le troisième et dernier pilier relatif à la transparence vis-à-vis des marchés peut aussi jouer un rôle important. Les organes délibérants pourront disposer de rapports sur la continuité de leurs activités, l'article 43 du CRBF 97/02 le suggère et le CRBF 98/02 le demandait trimestriellement pour le passage à l'an 2000. Les établissements sont libres de communiquer sur la qualité de leurs PCA et donc sur leur robustesse. Ensuite il sera de la responsabilité des analystes et opérateurs de marché de composer leur jugement en tenant compte de ces éléments qualitatifs qui témoignent de la pérennité des entreprises.

Les exigences de Bâle II devraient sensiblement faire avancer les pratiques de contrôle et de suivi des risques opérationnels dans les banques, jusqu'à conduire, comme pour les risques du métier bancaire que sont les risques de crédit et de marché, à la construction de modèles mathématiques alimentés par des statistiques rigoureuses. Il est intéressant de noter que ces risques opérationnels, tels qu'ils sont définis à Bâle, ne relèvent pas des seuls métiers bancaires, toute entreprise pouvant s'en préoccuper et se livrer aux mêmes contrôles, suivis et investissements de protection.

Un secours global des systèmes d'information

Sans attendre la mise en place de la réforme Bâle II prévue pour fin 2006, le modèle actuel de continuité des systèmes d'information devrait être renforcé [4]. Les passages en secours, application par application, qui montrent leurs limites, pourraient être abandonnés au profit d'un secours global entre un centre informatique et son « clone », maintenus dans des états strictement identiques. À terme, comme pour les chemins empruntés dans un réseau de télécommunications, les sites informatiques constituant un ensemble robuste devraient pouvoir être utilisés de manière indifférenciée. Ces qualités des systèmes de traitement de l'information, de déconcentration et substituabilité, devraient se retrouver dans les autres ressources mises en œuvre : humaines, pour les décisions et le savoir-faire, immobilières et chez les fournisseurs.

Concernant les fournisseurs, comme pour le passage à l'an 2000, il est conseillé qu'ils disposent eux-mêmes de plans de continuité cohérents avec ceux de leurs commanditaires. Les situations de monopole de place doivent être analysées, et les sous-traitances ne pas être un obstacle aux divers contrôles. Une révision du règlement 97/02 pourrait donc englober à la fois la question de la robustesse et celle de l'externalisation. Une telle évolution apparaît à la fois possible et utile. ■

1 L'Institut français de l'audit et du contrôle interne (IFACI) a organisé le 29 janvier 2003 un colloque sur le thème des plans de continuité.
2 Toujours en ligne sur le site internet de la Banque de France www.banque-France.fr.
3 Principe n° 7 de son rapport de juillet 2002 disponible à l'adresse suivante : www.bis.org/publ/bcbs.htm.
4 Par exemple, les obstacles techniques concernant la distance entre un centre de calcul et son secours en « *mirorring* » c'est-à-dire avec des données mises à niveau en temps réel, devraient tomber pour offrir un ordre de distance très supérieur : un secours à 200 km couvre des scénarios bien plus graves qu'un secours à 20 km.