AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DE LA CONTINUITÉ DES ACTIVITÉS

Avril 2010

TABLE DES MATIÈRES

Introduction

Le secteur financier est constitué d'une multitude d'interconnexions entre les différents marchés, systèmes, participants et fournisseurs de services. Une perturbation, un ralentissement ou une interruption des activités d'une institution financière ou d'un de ses fournisseurs de services, dus à des incidents opérationnels, pourraient compromettre sa capacité à respecter ses engagements vis-à-vis de sa clientèle et de ses partenaires et pourraient même, dans certains cas, perturber le système financier par effet de contagion. Compte tenu de ces interdépendances et de la complexité du fonctionnement du secteur financier, les institutions financières devraient se doter de pratiques de gestion saine et prudente afin d'assurer la continuité de leurs activités à la suite d'un incident opérationnel. La gestion de la continuité des activités constitue une priorité au chapitre de la saine gestion du risque opérationnel.

La gestion de la continuité des activités consiste à mettre en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer l'institution financière tels les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'institution et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

La présente ligne directrice a pour objectif d'énoncer les attentes de l'Autorité en matière de gestion de la continuité des activités. Les diverses lois sectorielles administrées par l'Autorité habilitent[1] cette dernière à donner des lignes directrices aux institutions financières pouvant porter sur toute pratique de gestion saine et prudente.

Les principes de gestion de la continuité des activités proposés par l'Autorité s'inspirent du cadre de référence[2] adopté par le ministère de la Sécurité publique au Québec. Ce cadre propose une démarche collective afin d'assurer la cohérence et la complémentarité de la gestion de la continuité. Cette démarche interpelle entre autres les instances gouvernementales, les organismes de santé et toute autre organisation ou institution fournissant des produits ou des services essentiels.

Cette ligne directrice s'inspire également des principes directeurs du Comité de Bâle sur le contrôle bancaire[3], de l'Association internationale des contrôleurs d'assurance[4] et du Joint Forum[5] relativement aux saines pratiques de gestion du risque opérationnel et de gestion de la continuité des activités.

1 *Loi sur les assureurs*, RLRQ, c. A-32.1, article 463; *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, article 565.1; *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, article 42.2; *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02, article 254.

2 GOUVERNEMENT DU QUÉBEC, MINISTÈRE DE LA SÉCURITÉ PUBLIQUE. Gestion des risques en sécurité civile, 2008. GOUVERNEMENT DU QUÉBEC, MINISTÈRE DE LA SÉCURITÉ PUBLIQUE. Approche et principes en sécurité civile, 2008.

3 COMITÉ DE BÂLE SUR LE CONTRÔLE BANCAIRE, BANQUE DES RÈGLEMENTS INTERNATIONAUX. Saines pratiques pour la gestion et la surveillance du risque opérationnel, février 2003.

4 ASSOCIATION INTERNATIONALE DES CONTRÔLEURS D'ASSURANCE. Principes de base en matière d'assurance et méthodologie, octobre 2003.

5 JOINT FORUM. High-level principles for business continuity, August 2006.

1. Continuité et reprise des activités

Aux fins de l'application de la présente ligne directrice, la gestion de la continuité des activités se définit comme étant un processus issu d'une stratégie et d'une politique, et des procédures visant à assurer la continuité et la reprise des activités critiques d'une institution financière à la suite d'un incident de nature opérationnelle. Les activités critiques d'une institution sont celles dont la perturbation, le ralentissement ou l'interruption pendant une certaine période auraient des répercussions importantes sur le fonctionnement de l'institution financière. En plus des répercussions importantes que peut avoir un incident, des impacts à l'égard des clients et des fournisseurs pourraient affecter la situation financière de l'institution et, ultimement, porter atteinte à sa réputation.

Les incidents opérationnels correspondent aux événements qui engendrent une perturbation, un ralentissement ou une interruption des activités critiques de l'institution et qui occasionnent des pertes financières ou une atteinte à sa réputation. Ces incidents pourraient être attribuables aux procédures propres à l'institution, ses ressources humaines et ses systèmes internes ou à des événements extérieurs comme les catastrophes naturelles, les incendies, les pannes d'électricité ou de télécommunications, les dysfonctionnements informatiques, le piratage, la malveillance, le terrorisme, les pandémies, etc.

Dans cette optique, l'institution financière est appelée à se doter d'un plan de continuité des activités (« PCA ») élaboré de façon rigoureuse afin d'assurer un niveau de préparation optimal aux incidents opérationnels majeurs. Dans les faits, le PCA est un plan d'action écrit qui définit les procédures et détermine les ressources nécessaires à la continuité et à la reprise des activités d'une institution.

2. Gestion saine et prudente de la continuité des activités

L'Autorité reconnaît que le choix du processus de gestion de la continuité des activités par l'institution financière dépend de plusieurs facteurs tels que sa taille, sa nature et la complexité de ses activités. Malgré les différents processus adoptés par les institutions financières, un processus efficace de gestion de la continuité des activités devrait s'appuyer sur les principes proposés ci-après, tels qu'une formulation claire de la stratégie de continuité et une implication de la haute direction et du conseil d'administration.

Le processus de gestion de la continuité des activités devrait également tenir compte de la nature et de l'importance des incidents opérationnels identifiés par l'institution. La ligne directrice ne vise que les incidents opérationnels majeurs.

Dans la détermination de l'étendue de sa gestion de la continuité, l'institution pourrait s'appuyer sur une approche basée sur les risques. Cette approche permet d'évaluer les différents incidents sur la base, notamment de leur probabilité d'occurrence et de leur sévérité, et d'établir des priorités de traitement. Cette priorisation repose sur la durée nécessaire à la reprise des activités et l'importance des effets que causerait leur interruption. L'institution pourrait déterminer alors des niveaux de services minimaux et des durées d'interruption tolérables. L'impossibilité d'assurer l'offre de produits et de services essentiels peut avoir des conséquences graves sur la réputation de l'institution. La gestion de la continuité des activités constitue un moyen efficace permettant de relever ce défi.

Le présent document propose des principes qui favorisent une gestion rigoureuse et efficace de la continuité des activités des institutions financières en fonction d'une démarche systématique et structurée. Ces principes visent également à favoriser l'utilisation d'une approche globale, permanente et intégrée dans la gestion de risques de l'institution financière.

Essentiellement, les principes proposés portent sur l'organisation de la gestion de la continuité, l'identification des incidents opérationnels majeurs, l'évaluation de leurs impacts sur les activités critiques de l'institution et la planification de la gestion de la continuité.

3. Cadre général de la gestion de la continuité des activités

Principe 1 : Responsabilités du conseil d'administration et de la haute direction

> L'Autorité s'attend à ce que la gestion de la continuité des activités fasse partie intégrante de la gestion intégrée des risques de l'institution financière, dont le conseil d'administration et la haute direction sont ultimement responsables.

L'Autorité s'attend à ce que les rôles et les responsabilités liés à la gestion de la continuité des activités soient clairement définis et adéquatement documentés. La Ligne directrice sur la gouvernance[6] propose des principes en matière de gestion saine et prudente que l'institution financière devrait considérer a priori en regard des spécificités de la gestion de la continuité des activités. Dans ce cadre, le conseil d'administration devrait notamment :

- approuver la stratégie et la politique de continuité des activités;
- nommer un responsable de la gestion de la continuité des activités parmi les membres de la haute direction.

Les rôles et responsabilités de la haute direction portent notamment sur les éléments suivants :

- assurer l'efficacité de la gestion de la continuité et la reprise des activités perturbées ou interrompues dans des délais raisonnables;
- créer et promouvoir une culture organisationnelle qui accorde une place prépondérante à la gestion de la continuité;
- approuver le PCA;
- s'impliquer, en cas d'incidents majeurs affectant la continuité des activités, en adaptant les directives préétablies aux imprévus rencontrés;
- assurer la survie financière de l'institution;
- soumettre périodiquement des rapports au conseil d'administration sur la capacité de l'institution financière à répondre à un incident;
- allouer les ressources nécessaires à l'élaboration et la mise en place du PCA.

La haute direction devrait former un comité de gestion de la continuité des activités. Ce comité pourrait être responsable de l'élaboration, de la planification, de la vérification et de la mise à jour du PCA. Il pourrait en assurer également la mise en œuvre, en plus de coordonner les activités et de superviser l'élaboration du PCA. Dans certains cas, la désignation d'un seul responsable pourrait être suffisante. Toutefois, il ne serait pas nécessaire de désigner un responsable lorsque les lois prévoient des structures ou des comités qui peuvent prendre en charge cette responsabilité.

Principe 2 : Stratégie, politique et procédures

> L'Autorité s'attend à ce que l'institution financière dispose d'une stratégie lui permettant d'assurer la continuité des activités critiques et la reprise des activités perturbées ou interrompues, et ce, dans des délais raisonnables.

[6] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*.

La gestion de la continuité des activités devrait faire partie intégrante de la gestion au jour le jour de l'institution financière. L'institution financière devrait élaborer une stratégie de continuité des activités et mettre en place une politique et des procédures qui traduisent cette stratégie sur le plan opérationnel en couvrant notamment les éléments suivants :

- la mise en place d'un comité de gestion de la continuité impliquant la haute direction;
- la définition des rôles et responsabilités de toutes les personnes qui peuvent être impliquées;
- la mise en place de plans de délégation de pouvoirs, afin de répondre efficacement aux imprévus et de réduire les questionnements quant à l'attribution des responsabilités en cas de perturbation, de ralentissement ou d'interruption des activités critiques de l'institution;
- l'identification des incidents opérationnels majeurs susceptibles d'affecter l'institution financière;
- l'identification des activités critiques;
- l'évaluation de l'impact des incidents opérationnels majeurs sur les activités critiques;
- le développement des objectifs de continuité;
- l'élaboration d'un PCA détaillé qui décrit les actions à entreprendre;
- la coordination des actions de l'institution financière avec celles entreprises par les instances gouvernementales ou les fournisseurs de services;
- la mise en place d'un programme de formation et de sensibilisation des employés impliqués;
- l'élaboration d'un plan de communication;
- la vérification de la fiabilité du PCA et sa mise à jour.

4. Identification et évaluation des incidents opérationnels majeurs

Principe 3 : Identification des incidents opérationnels majeurs

> L'Autorité s'attend à ce que l'institution financière identifie les incidents opérationnels majeurs susceptibles de perturber, de ralentir ou d'interrompre ses activités critiques.

Aux incidents opérationnels habituellement identifiés comme les catastrophes naturelles, les pannes informatiques, les attaques terroristes et d'autres actes délibérés ou accidentels, s'ajoutent des incidents nouveaux liés à l'automatisation accrue, au recours croissant à l'impartition et à l'interdépendance des systèmes financiers. Certains incidents, tels qu'une pandémie d'influenza, ont la particularité d'avoir des répercussions directes sur les ressources humaines alors que la majorité des incidents opérationnels entraînent une détérioration ou un dysfonctionnement des systèmes et des infrastructures physiques.

Les incidents opérationnels majeurs peuvent engendrer une ou plusieurs des conséquences suivantes : la dégradation ou la destruction des infrastructures physiques et des systèmes, l'indisponibilité ou la perte des ressources humaines, l'accès restreint aux zones affectées, les pertes financières et l'atteinte à la réputation. Ces incidents sont également susceptibles de générer des pertes financières considérables. Ils pourraient même porter atteinte à la réputation de l'institution financière. Ces incidents peuvent ultimement affecter l'ensemble du système financier.

L'institution financière devrait donc déterminer les incidents susceptibles de l'affecter et en évaluer l'impact sur son profil de risque. Parmi les critères permettant l'identification des incidents opérationnels majeurs et l'établissement des priorités pour en assurer la gestion, on retient principalement :

- l'intensité;
- la probabilité d'occurrence;
- la localisation de l'incident et son étendue;
- la vitesse d'évolution;
- la durée de l'impact;
- le moment où l'incident est susceptible de survenir;
- la prévisibilité;
- la possibilité de maîtrise ou de contrôle.

L'institution devrait également considérer le fait que la manifestation de certains incidents serait susceptible de provoquer le déclenchement d'incidents secondaires. Par exemple, un séisme pourrait provoquer des incendies en raison des fuites de gaz.

Principe 4 : Identification des activités critiques

> L'Autorité s'attend à ce que l'institution financière identifie ses activités critiques à la continuité des activités, leur concentration sur un même site, leur interdépendance ainsi que leur dépendance quant au même système, personnel et fournisseurs de services.

D'une part, l'institution financière devrait s'assurer que les prestations des fournisseurs de services dont dépendent ses activités critiques seront disponibles. Par exemple, l'institution devrait tester régulièrement les systèmes de communication entre ses sites et ceux de ses fournisseurs de services. Dans la même optique, l'institution financière devrait vérifier que les risques liés à ses activités imparties ne compromettent pas la continuité de ses activités. Ainsi, l'institution devrait s'assurer que ses fournisseurs de services disposent d'un PCA fiable et voir, le cas échéant, à adapter son propre PCA selon les risques résiduels identifiés[7].

D'autre part, certaines institutions financières peuvent avoir choisi de centraliser certaines de leurs activités critiques et activités de support (p. ex. : l'informatique). Cette centralisation est susceptible d'accroître les risques d'interruption des activités situées sur un même site ou dépendantes de ce site en cas d'incidents. Par conséquent, l'institution financière devrait envisager de mettre en place les mesures nécessaires afin d'atténuer les risques liés à la concentration de ses activités. Elle pourrait, à titre d'exemple, prévoir des sites de reprise.

Principe 5 : Évaluation des impacts sur les activités critiques

> L'Autorité s'attend à ce que l'institution financière évalue les impacts des incidents majeurs sur ses ressources, son fonctionnement et son environnement et détermine les mesures à prendre découlant de cette évaluation.

Dans son évaluation des impacts des incidents opérationnels majeurs sur les activités critiques, l'institution financière devrait notamment considérer les éléments suivants :

- les effets sur les infrastructures, systèmes et ressources matérielles dont dépend l'institution financière pour la réalisation de ses activités quotidiennes, telles que l'électricité, les télécommunications, etc.;
- les effets sur la population liée géographiquement et économiquement à l'institution financière (p. ex. : son personnel, ses clients, ses fournisseurs, ses partenaires, etc.);
- les impacts financiers et économiques.

L'institution financière devrait également considérer le risque systémique dans l'évaluation d'impact sur son environnement. Dans le cas de plusieurs incidents opérationnels (p. ex. : les catastrophes naturelles, la pandémie d'influenza, etc.), la survenance d'un risque systémique doit être prise en compte puisque les conséquences de ces incidents pourraient avoir une étendue géographique vaste. Cette étendue peut être accentuée par l'interconnexion des marchés financiers et l'interdépendance des systèmes économiques.

Dans son évaluation des impacts, l'institution financière devrait estimer la disponibilité des ressources nécessaires au fonctionnement de chaque activité critique (les ressources humaines et matérielles, les processus des fournisseurs de services, les réseaux de télécommunication, etc.). Elle devrait également prendre en considération les mesures d'atténuation qu'elle a mises en place (p. ex. : sites de reprises, plans de sauvegarde des données, etc.).

L'évaluation des impacts devrait permettre à l'institution financière d'anticiper les perturbations, les ralentissements et les interruptions possibles de ses activités critiques. Sur cette base, l'institution financière devrait fixer ses objectifs de continuité et de reprise, dont entre autres :

- gérer les conséquences immédiates d'un incident;
- assurer la continuité des activités critiques;
- maintenir un niveau de service approprié;

[7] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion des risques liés à l'impartition.*

- minimiser la durée d'interruption à un niveau acceptable pour l'institution.

Les objectifs de l'institution devraient être établis en considérant ce qui est prioritaire en cas d'incidents majeurs. Ces priorités pourraient notamment être la protection des employés, la survie financière de l'institution, la conformité aux lois et règlements en vigueur et le maintien des services essentiels aux clients.

L'allocation des ressources ne saurait être efficace sans des objectifs clairs et précis. De façon générale, ces ressources se font rares en cas d'incidents majeurs. Les objectifs fixés par l'institution permettront l'élaboration d'un PCA adapté au profil de risque de l'institution.

5. Développement et implantation du plan de continuité des activités

Principe 6 : Planification de la continuité des activités

> L'Autorité s'attend à ce que l'institution financière développe et implante un PCA qui documente les actions à entreprendre en cas d'incident opérationnel majeur ayant un impact sur les activités critiques.

Le PCA est la composante principale et tangible d'une saine gestion de la continuité des activités d'une institution financière. Dans cette optique, celui-ci devrait être clair, pratique, vérifié et mis à jour régulièrement. Il devrait également être accompagné d'un plan de communication.

L'institution financière devrait planifier la continuité et la reprise de ses activités en mettant en place des mesures d'intervention adéquates. Ces mesures devraient décrire en détail les façons et les moyens d'assurer la continuité des activités critiques à un niveau de service minimal, avec une durée d'interruption tolérable, notamment lorsque les ressources habituelles ne sont pas disponibles. À cet égard, l'institution financière devrait élaborer son PCA afin de consigner les mesures qu'elle compte adopter en se basant sur un ensemble d'éléments à caractère :

- organisationnels : développement de politiques, de procédures, de plans d'action, de mesures d'urgence, d'une vérification de la fiabilité, de la mise à jour, etc.;
- humains : sensibilisation, formation, etc.;
- technologiques : logiciels, matériels, bases de données, réseaux, etc.;
- physiques et matériels : infrastructures, sites de reprise, etc.

Les sous-sections ci-après élaborent sur certains de ces éléments.

5.1 Atténuation de la menace des incidents opérationnels majeurs

L'atténuation des risques est un processus permanent qui doit se poursuivre même si le PCA n'est pas activé. Par exemple, si une institution a besoin d'électricité pour poursuivre ses activités critiques, elle peut atténuer le risque d'une panne d'électricité de courte durée en installant des génératrices.

5.2 Sites de reprise

L'institution devrait avoir accès à un ou des sites de reprise au cas où elle perdrait ses sites principaux ou ses biens matériels, les réseaux et applications des technologies de l'information. Le choix des sites de reprise devrait tenir compte de plusieurs facteurs, y compris de la nature des incidents opérationnels majeurs menaçant l'institution, du temps d'interruption acceptable et des coûts. L'institution financière devrait également tenir compte de ces facteurs pour choisir les sites qui correspondent à ses objectifs de continuité et ses niveaux de tolérance aux risques.

L'emplacement des sites de reprise devrait être suffisamment éloigné du site principal afin d'éviter qu'ils ne soient soumis aux mêmes perturbations que les sites principaux. Ainsi, les sites de reprise ne devraient pas dépendre des mêmes systèmes et infrastructures que le site principal et par conséquent disposer de réseaux électriques et de télécommunication indépendants.

5.3 Programmes de sensibilisation et de formation

Afin d'instaurer une culture de gestion de la continuité au sein de l'institution, il est nécessaire d'informer et de sensibiliser les employés quant à leurs responsabilités dans le cadre du PCA. Pour ceux qui ont des responsabilités directes, des formations devraient être fournies afin de s'assurer que ces employés maîtrisent et comprennent les directives fixées par le PCA et qu'ils sont en mesure de les appliquer adéquatement.

5.4 Communication

La réussite du déploiement du PCA est tributaire d'une communication cohérente, claire et efficace afin, par exemple, de contenir les rumeurs. Ainsi, une bonne organisation de la communication permettra de maintenir le contact avec les médias, les services d'urgence, les partenaires, les fournisseurs et, par conséquent, de rassurer les employés et les clients.

Principe 7 : Vérification de la fiabilité du PCA et mise à jour

> L'Autorité s'attend à ce que l'institution financière vérifie périodiquement la fiabilité de son PCA. L'Autorité s'attend également à ce que le processus de gestion de la continuité des activités soit un processus dynamique prenant en charge les changements qui affectent l'institution financière, ses tiers et son environnement.

Les changements sur le plan des technologies, des processus, des rôles et des responsabilités des employés peuvent affecter la fiabilité du PCA. Il est donc important de vérifier régulièrement sa fiabilité. L'institution financière devrait s'assurer que le déploiement du PCA lui permette de poursuivre ses activités critiques de façon efficace et efficiente.

Selon la nature et la complexité des activités critiques, des ressources et du temps disponibles, l'institution financière pourrait procéder à des exercices par modules, à différents intervalles et sur une base régulière. La haute direction et les employés qui seront impliqués dans la gestion de la continuité devraient participer à ces exercices afin de se familiariser avec les rôles et responsabilités qui leur ont été attribués dans le cadre du PCA. Les exercices devraient notamment permettre une vérification :

- des composantes distinctes du PCA;
- de la connexion et le fonctionnement des outils, des systèmes et des sites de reprise;
- des aspects qualitatifs (temps nécessaire à la reprise des activités) et quantitatifs (capacité de la reprise des activités);
- de la validité des hypothèses retenues lors de la planification;
- de la coordination avec les partenaires d'affaires et les instances gouvernementales.

Afin de disposer d'une image d'ensemble de la stratégie de continuité des activités, l'institution devrait mener des exercices intégrant les principales composantes du PCA. L'institution financière pourrait également accroître progressivement le niveau de difficulté des exercices en ajoutant de nouveaux scénarios. Un niveau de difficulté accru permettrait une meilleure vérification de la fiabilité du PCA.

À la fin de chaque exercice, un rapport devrait être rédigé. Selon les résultats obtenus, les solutions ou les correctifs nécessaires devraient être intégrés afin de produire une version amendée du PCA.