



**Consultation sur le projet de
« Ligne directrice sur la gestion de la
continuité des activités »**

Commentaires présentés à

L'Autorité des marchés financiers

Le 30 octobre 2009

Le Bureau d'assurance du Canada

Le Bureau d'assurance du Canada (BAC) est l'organisme qui représente les sociétés privées d'assurance de dommages. L'industrie de l'assurance assume un rôle de premier plan dans l'économie québécoise en permettant à la population de se protéger contre des sinistres pouvant avoir un impact important sur sa sécurité financière. En fait, l'assurance de dommages crée un filet de sécurité qui favorise la poursuite de l'innovation et de l'investissement. Elle appuie une économie dynamique et vigoureuse en suscitant une plus grande tranquillité d'esprit à l'égard de bon nombre des risques qui caractérisent la vie moderne.

L'industrie de l'assurance de dommages génère près de 23 000 emplois directs dans le secteur privé. En 2008, les assureurs de dommages ont versé à leurs assurés québécois plus de 4,7 milliards de dollars afin de les indemniser à la suite d'une perte accidentelle subie par leur véhicule, leur habitation, leur commerce ou une poursuite en responsabilité civile.

Également, l'Industrie contribue à l'amélioration de la qualité de vie de la société québécoise par ses programmes de prévention des sinistres, d'éducation des consommateurs et de prévention du crime.

Introduction

Nous souhaitons mentionner que les assureurs, tant à charte fédérale que provinciale, sont déjà conscientisés au besoin de gestion de la continuité de leurs activités dans le cadre d'une gestion saine et prudente de leurs risques et qu'ils ont tous déjà mis en place des mesures à cet effet, donc sont d'accord avec les grands principes énoncés dans cette ligne directrice.

Commentaires du BAC sur la ligne directrice

Commentaire général

Nous souhaitons que les définitions des expressions clés utilisées dans tout le document soient regroupées dans le Champ d'application et que la terminologie utilisée soit uniformisée. Ainsi, à certains endroits dans le texte, on fait référence à des « incidents majeurs », à des « activités critiques », tandis qu'à d'autres endroits on mentionne plutôt des « incidents opérationnels majeurs » et « incidents opérationnels ».

Commentaires spécifiques

Introduction (page 4)

Nous sommes d'avis que le plan de continuité exigé dans la ligne directrice doit viser seulement les activités critiques de l'institution qui peuvent être impactées par des incidents opérationnels majeurs. Il est clairement précisé à la page 7, point 2, Gestion saine et prudente de la continuité des activités, que « la ligne directrice ne vise que les incidents opérationnels majeurs » contrairement à ce qui est mentionné au deuxième paragraphe de la section Introduction.

Dans le cadre de la gestion des risques, les assureurs de dommages doivent effectivement identifier les incidents opérationnels majeurs pouvant affecter leurs activités critiques et mettre en place des mécanismes pour assurer la continuité de leurs activités d'affaires pour répondre adéquatement à leurs clientèles et garantir leur santé financière.

Entrée en vigueur et processus de mise à jour (page 6)

Comme il l'a été fait dans les autres lignes directrices publiées en 2009 par l'Autorité, nous souhaitons qu'il soit clairement indiqué que les institutions financières disposeront de 24 mois pour se conformer à la ligne directrice sur la gestion de la continuité des activités à partir de sa publication. Selon nous, ce délai est raisonnable et devrait laisser suffisamment de temps aux institutions financières pour s'y conformer.

3. Cadre général de la gestion de la continuité des activités**Principe 1 : Responsabilités de la haute direction et du conseil d'administration** (page 8)

Dans la section des responsabilités du conseil d'administration, relativement aux points 1 « valider la stratégie de continuité à adopter » et 2 « approuver le PCA », nous considérons que le conseil d'administration pourrait approuver la politique de la continuité des affaires de l'entreprise, mais qu'il appartient plutôt à la haute direction d'approuver le PCA qui constitue le plan d'application de la politique de la continuité des affaires de l'entreprise. Ainsi, le conseil d'administration pourrait émettre ses exigences à la haute direction sur les grands fondements du PCA qui seraient exprimés dans la politique et n'aurait pas à s'impliquer dans les opérations de la société, ce qui n'est pas son rôle.

En effet, le PCA doit s'appliquer à divers degrés à tous les secteurs de l'entreprise, contenir en détail toutes les mesures de contrôles et être modifié constamment pour répondre aux besoins changeants de l'environnement, des opérations et possiblement des lois qui les gouvernent. Donner cette responsabilité au conseil d'administration l'amènerait à agir à un niveau beaucoup trop opérationnel.

Dans les responsabilités de la haute direction :

Ajouter la responsabilité : allouer les budgets nécessaires à l'élaboration et la mise en place du PCA.

Le dernier point de cette section, en page 9, devrait être clarifié et se lire comme suit : « soumettre périodiquement des rapports au conseil d'administration sur la capacité de l'institution financière à répondre à un incident. » au lieu de « soumettre périodiquement des rapports au conseil d'administration sur le niveau de préparation de l'institution financière. »

Principe 2 : Stratégie, politique et procédure (page 9)

Des modifications devraient être apportées dans l'énumération des items du Principe 2. La politique est un énoncé de grands principes indiquant la ligne de conduite adoptée pour la gestion de ses affaires. Pour sa part, la stratégie est l'art de planifier et de coordonner un ensemble d'opérations en vue d'atteindre un objectif (conception d'actions coordonnées). Finalement, une procédure est l'ensemble des règles à suivre pour parvenir à un résultat¹. Par conséquent, dans la logique des choses, l'institution doit adopter une politique qui contiendra les grands principes d'une stratégie d'application de la politique. Les procédures de mise en place découleront de la politique et ses stratégies.

Partant du principe que l'on passe du plus général au plus particulier, nous devrions plutôt lire Politique, stratégie et procédure.

¹ Marie-Éva DE VILLERS, *Multi Dictionnaire de la langue française*, Les Éditions Québec Amérique, 2003

4. Identification et évaluation des incidents opérationnels majeurs

Principe 3 : Identification des incidents opérationnels majeurs (page 10)

Dans le dernier paragraphe de la page 10, le mot « éventail » est trop général et devrait être remplacé par « liste d'incidents majeurs » puisqu'il laisse supposer que tous les types d'incidents devraient être répertoriés ainsi qu'une stratégie développée pour chaque incident. Comme le titre l'indique, il s'agit des incidents opérationnels majeurs ayant un impact sur les activités critiques de l'institution et non tous les événements possibles qui pourraient survenir ayant des impacts ou non sur les activités de l'assureur.

À ce titre, le premier point « l'intensité » devrait plutôt référer à « l'impact ». Nous croyons que l'Autorité fait plutôt référence aux impacts d'un incident opérationnel majeur sur les opérations critiques de l'institution au lieu de l'intensité.

Principe 4 : Identification des activités critiques (page 11)

Le principe énoncé dans l'encadré devrait préciser qu'il s'agit des « activités critiques à la continuité des affaires » soit celles qui ont un impact majeur sur le fonctionnement de l'institution financière. Une liste trop exhaustive sur toutes les activités potentiellement perturbées pour l'organisation ne serait pas utile.

Premier paragraphe, dernière phrase « Ainsi, l'institution devrait s'assurer que ses fournisseurs de services disposent d'un PCA fiable et régulièrement vérifié et voir à adapter son propre PCA le cas échéant, selon les risques résiduels identifiés », comme prévu dans la directive sur l'impartition, l'institution financière peut exiger dans ses contrats que le fournisseur de services majeurs dispose d'un plan de relève qui corresponde à ses besoins, mais il ne peut en demander davantage.

Principe 5 : Évaluation des impacts sur les activités critiques (page 12)

Dans l'encadré, « incidents majeurs » devrait plutôt être « incidents opérationnels majeurs ».

Le dernier point de la page 12 « garantir une durée d'interruption raisonnable » est ambigu, car cet objectif de continuité s'applique à toutes les activités de l'institution. Il serait plus exact de dire « minimiser la durée d'interruption à un niveau acceptable pour l'organisation ».

Principe 6 : Planification de la continuité des activités (pages 13 et 14)

Dans l'énoncé de principe, il devrait être précisé qu'il s'agit « d'incident opérationnel majeur ayant un impact sur les activités critiques. »

Toute la section Sites de reprise est selon nous beaucoup trop détaillée et ne relève pas d'une ligne directrice, mais plutôt d'une définition. Nous recommandons de placer ces commentaires en annexe sous forme informative. De plus, nous tenons à souligner qu'il existe d'autres moyens de relève, comme les intersites par exemple, alors qu'une succursale ou une autre place d'affaires vient en relève à une autre.

Principe 7 : Vérification de la fiabilité du PCA et mise à jour (page 15)

Dans le titre, l'énoncé de principe et tout le texte utilisent le terme « vérification » qui pourrait porter à confusion. Lorsqu'il est fait mention de vérification, le lecteur pourrait penser à vérification externe alors que ce n'est pas le cas. Le titre du principe pourrait être modifié pour « Exercice (ou maintenance) du PCA et mise à jour ». Dans cette optique, l'institution financière met son PCA à jour et est en mesure de s'assurer que son plan correspond le plus possible à la réalité.

Dans l'encadré, au lieu de « ...que l'institution financière vérifie périodiquement... » on devrait lire « ...l'institution financière s'assure périodiquement de la... ».

Le premier point « toutes les composantes distinctes du PCA » devrait plutôt se lire « les principales composantes du PCA ». Pour certaines institutions financières qui sont présentes dans plusieurs lieux physiques à travers le pays, un tel exercice qui comprend toutes les composantes est utopique. La lourdeur et la complexité d'un tel exercice sont impensables.

Au quatrième point « la validité des hypothèses de planification », la notion d'hypothèses fait-elle référence aux scénarios? Une clarification s'impose pour cet item.

À la page 16, dans le premier paragraphe, on fait mention « des exercices à un niveau centralisé ». L'Autorité pourrait-elle être plus claire sur ce point puisqu'il y a confusion en ce qui concerne cet aspect? Veut-on parler de test intégré? Fait-on référence à par région, par opération, par secteur ou par site?

De plus, dans la même phrase, on fait référence à « tous les modules », une uniformisation est appropriée puisque dans tout le document on parle des principales composantes du PCA.

Surveillance des pratiques de gestion saine et prudente

Comme dans les autres directives, les pouvoirs de vérification de la conformité par l'Autorité doivent faire l'objet d'un point séparé. Il devrait être Point ou Section 6.

Conclusion

Le BAC remercie l'Autorité des marchés financiers de lui offrir la possibilité de commenter au nom de l'Industrie le projet de ligne directrice sur la gestion de la continuité des activités.