Canadian Institute of Actuaries | Institut canadien des actuaires

5 février 2024

Bureau du surintendant des institutions financières (BSIF)
resilience@osfi-bsif.gc.ca

Objet : Réponse de l'ICA à la version à l'étude de la ligne directrice E-21 – Résilience opérationnelle et gestion du risque opérationnel

L'Institut canadien des actuaires (ICA) est heureux de présenter ses commentaires sur cette importante version à l'étude de la ligne directrice.

L'ICA apporte son soutien au BSIF concernant l'élargissement de sa ligne directrice E-21 existante afin de mettre l'accent sur la résilience opérationnelle en plus de la gestion des risques opérationnels. Nous encourageons le BSIF à améliorer le libellé tout au long du document afin de souligner que la lignes directrice est fondée sur des principes. Nous suggérons également que le BSIF reconnaisse explicitement que l'application de la ligne directrice devrait être fondée sur le risque, ce qui permettrait aux institutions financières fédérales (IFF) d'adapter l'application à leurs circonstances particulières.

A. Vue d'ensemble

Nous sommes heureux de constater que l'accent est mis sur les activités essentielles, mais nous avons remarqué que les attentes s'étendent parfois à l'ensemble des activités. La notion d'application fondée sur le risque devrait être ajoutée et devrait compléter une approche fondée sur des principes afin de permettre la reconnaissance des opérations essentielles ou à risque élevé, y compris le fait qu'il peut y avoir des fonctions au sein des opérations essentielles qui ne sont pas elles-mêmes essentielles.

A.3 Application et principe de proportionnalité

Nous sommes heureux du recours au principe de proportionnalité, nous ne savons pas toutefois quelles sont les attentes à l'égard des institutions de plus petite taille qui offrent des services ou des produits uniques. Le libellé actuel de la version à l'étude laisse entendre qu'il y a des cas où les produits ou les services offerts par une institution de plus petite taille sont si importants qu'une perturbation de cette institution pourrait entraîner la faillite du système financier ou de l'économie. Le BSIF pourrait envisager de fournir un exemple d'une telle situation, car il n'est pas évident au début quel scénario pourrait donner lieu à ce résultat.

La version à l'étude de la ligne directrice utilise un libellé relatif à l'interrelation, mais ne fournit pas d'exemples. Nous reconnaissons que les services bancaires, tels que Interac et d'autres processus de paiement, sont essentiels au système financier, à l'économie et aux autres IFF,

le BSIF pourrait aussi envisager d'inclure un exemple de services propres à l'assurance qui seraient considérés comme essentiels au système financier ou à l'économie.

A.4 Définitions

La définition de « résilience opérationnelle » comprend une référence explicite au risque lié aux technologies et au cyberrisque. La résilience opérationnelle nécessite que **tous** les éléments opérationnels (personnes, processus, etc.) fonctionnent de manière à soutenir la livraison de produits et de services, y compris ceux jugés essentiels. Il n'est pas clair pourquoi le risque lié aux technologies et le cyberrisque sont explicitement mentionnés, alors que d'autres catégories de risques opérationnels ne le sont pas. Cela pourrait conduire à considérer d'autres éléments opérationnels comme étant moins importants.

La version à l'étude de la ligne directrice définit le « risque opérationnel » comme le risque de pertes attribuables au personnel, à une inadéquation ou à une défaillance des processus et des systèmes internes, ou à des événements extérieurs. Bien que nous comprenions qu'il s'agit d'une définition normalisée (utilisée par l'Association internationale des contrôleurs d'assurance, par exemple), nous préférerions que chaque IFF puisse utiliser sa propre définition qui reflète sa culture et son approche de communication, tout en conservant les éléments clés de la définition du BSIF. Par exemple, nous avons vu une définition légèrement modifiée, comme suit : « Le risque opérationnel est défini de façon générale comme le risque de pertes résultant d'erreurs humaines, de décisions, d'actions ou d'inaction, de processus et de systèmes internes inadéquats ou défaillants, ou d'événements externes ayant une incidence sur les activités de l'entreprise ».

La définition du risque lié aux données, telle que rédigée, laisse entendre qu'il peut y avoir des « personnes inadéquates ou défaillantes » à la manière des processus et des systèmes inadéquats et défaillants. Nous ne sommes pas certains quant à l'intention sous-tendant cette formulation et recommandons que le BSIF révise et réécrive cette définition.

Nous sommes heureux de constater que la définition de la « mise à l'essai de scénarios » concorde avec celle décrite dans la ligne directrice E-18 et nous estimons qu'un renvoi à la norme E-18 serait utile.

Nous recommandons d'inclure une définition de « scénarios graves, mais vraisemblables ». Par ailleurs, le BSIF pourrait envisager de mettre à jour la ligne directrice E-18 afin de saisir les éléments relatifs à la mise à l'essai de scénarios, puis de renvoyer à la ligne directrice E-18, le cas échéant.

Nous recommandons d'ajouter une définition des « fonctions centrales », même si nous notons que les structures organisationnelles des IFF peuvent varier considérablement.

Enfin, nous notons que même si les définitions mentionnées comprennent le risque lié aux données, elles n'incluent pas d'autres risques indiqués dans la version à l'étude de la ligne directrice et couverts également dans d'autres lignes directrices du BSIF.

A.6 Consignes connexes

Nous recommandons que cette liste soit élargie pour inclure le Bulletin E-5 relatif à la « Conservation et destruction des registres », la nouvelle ligne directrice « Intégrité et sécurité » et éventuellement la « version à l'étude de la ligne directrice E-23 – Gestion du risque de modélisation », bien que nous reconnaissions que cette dernière ligne directrice

n'en est qu'à ses premières étapes de consultation. Nous suggérons également de se référer à la ligne directrice B-3 « Saines pratiques et procédures de réassurance ». Bien que la ligne directrice B-3 soit largement axée sur le risque financier, il existe des éléments de risque opérationnel associés à la réassurance et il serait utile de souligner ce lien.

1.1 La haute direction est responsable de la résilience opérationnelle et de la gestion du risque opérationnel

Même si nous convenons qu'il devrait y avoir une appropriation et des responsabilités claires en matière de résilience opérationnelle et de gestion du risque opérationnel, ça reste plutôt vague comment le BSIF définit les « fonctions centrales ».

1.2 La résilience opérationnelle et la gestion du risque opérationnel sont intégrées au programme et aux rapports de gestion du risque d'entreprise de l'IFF

Dans la version à l'étude de la ligne directrice, on mentionne que la « résilience opérationnelle soit pleinement intégrée à son programme de gestion du risque d'entreprise, qui englobe le risque opérationnel, le risque lié aux technologies et le cyberrisque, le risque lié aux tiers et le risque lié aux données [...] ». Nous recommandons de supprimer toutes les références aux catégories de risque opérationnel dans cette affirmation. La ligne directrice comprend une définition du risque opérationnel. L'inclusion et l'exclusion de certaines catégories peuvent créer de la confusion et donner à penser que d'autres éléments du risque opérationnel sont moins importants. L'évaluation des catégories devrait être propre à chaque IFF en fonction de la nature de leurs activités.

1.3 Les secteurs d'activité et les fonctions centrales gèrent le risque et font l'objet d'une supervision indépendante et 1.3.2 Une supervision indépendante de la gestion du risque et de la conformité est assurée à l'égard de la résilience opérationnelle et de la gestion du risque opérationnel

Dans la présente section, il est fait mention des « fonctions centrales » et de la « fonction de supervision de la gestion du risque et de la conformité » séparément, ce qui semble indiquer que cette dernière ne fait pas partie des fonctions centrales. Il peut être utile de définir les fonctions centrales et de se reporter à la ligne directrice du BSIF sur la Gouvernance d'entreprise pour la référence à la gestion du risque et à la conformité en tant que fonctions de supervision. Notre interprétation est que les fonctions de supervision de la gestion du risque et de la conformité sont secondaires, tandis que les fonctions centrales sont principales. Il peut être utile de clarifier cette section.

De plus, le libellé laisse entendre que la supervision de la gestion du risque et de la conformité constitue une seule fonction. D'un point de vue pratique, ce n'est généralement pas le cas.

1.3.3 Une assurance indépendante est fournie

La ligne directrice précise que l'assurance indépendante devrait être fournie par la vérification interne ou une fonction semblable. Le BSIF peut-il fournir un exemple d'une fonction similaire?

2. Résilience opérationnelle

Nous sommes d'accord avec l'énoncé des résultats de cette section, mais nous suggérons de reconnaître que les fonctions au sein des opérations essentielles ne sont pas elles-mêmes toutes essentielles.

2.2.1 Un niveau de tolérance aux perturbations doit être établi pour chaque activité essentielle recensée

La version à l'étude de la ligne directrice introduit la notion de « tolérance aux perturbations » et suggère d'évaluer la capacité des IFF d'exercer leurs activités en respectant cette « tolérance » dans le cadre de l'analyse de scénarios. Nous constatons que les définitions fournies dans la version à l'étude diffèrent des pratiques de gestion du risque d'entreprise établies. Par exemple, l'ICA a publié un document d'appui à la pratique qui comprend des définitions de ces concepts. Nous suggérons d'inclure les définitions suivantes[1] tirées du document de l'ICA afin de mettre le lectorat en contexte :

> La **propension à prendre des risques** définit le niveau et le type de risque qu'une organisation est disposée à accepter pour atteindre ses objectifs. Elle s'exprime dans une série d'énoncés qualitatifs et quantitatifs qui décrivent la propension à prendre des risques par rapport aux bénéfices nets, au capital, aux liquidités et à d'autres mesures, le cas échéant.
>
> La **capacité de prendre des risques** est le niveau de risque maximal qu'une organisation peut accepter avant de manquer aux contraintes en matière de risque. Ces contraintes sont déterminées par les besoins en capital réglementaire et en liquidités, l'environnement opérationnel (infrastructure technique, capacités de gestion des risques, expertise) et les obligations envers les parties prenantes (déposants, titulaires de contrats, actionnaires, investisseurs dans un revenu fixe et organismes de réglementation). La tolérance au risque est limitée par la capacité de prendre des risques.
>
> La **tolérance au risque** est le niveau maximal de risque qu'une organisation est disposée et apte à accepter. Il s'agit de l'application pratique de la propension à prendre des risques, qui articule sur le plan opérationnel les énoncés de la propension à prendre des risques au moyen de mesures qualitatives ou quantitatives qui peuvent être surveillées et examinées
>
> La **tolérance au risque** est le niveau de risque maximal qu'une organisation est disposée à accepter et est en mesure d'accepter. Il s'agit de la demande pratique d'appétence au risque et de la mise en œuvre des énoncés d'appétence au risque au moyen de mesures qualitatives et/ou quantitatives qui peuvent être surveillées et examinées.
>
> Les **limites de risque** sont les mesures qualitatives et quantitatives qui répartissent la tolérance au risque d'une organisation entre les secteurs d'activité, les filiales, les catégories de risque, les concentrations de risque et d'autres niveaux, le cas échéant. Les limites de risque convertissent la tolérance au risque en limites au titre des mesures de surveillance du risque. Certaines limites de risque sont fermes; leur dépassement représente un niveau de risque inacceptable qui nécessite l'application de mesures correctives immédiates. Certaines sont souples et fournissent un signal de préalerte à mesure que le profil de risque approche des limites de risque.

[1] Ces définitions sont tirées du document d'appui à la pratique de l'ICA intitulé *Propension à prendre des risques*.

Le dépassement d'une limite souple incite la direction à déterminer si des mesures correctives sont nécessaires.

Nous notons que mesurer la perturbation en termes de durée ou d'unité de temps est normatif et limitatif. Les IFF devraient être en mesure d'établir une mesure adaptée à l'opération essentielle et aux risques connexes.

2.3.3 La fréquence et l'intensité des mises à l'essai sont proportionnelles au risque et à la criticité

Nous convenons que la fréquence et l'intensité des essais devraient être proportionnelles au risque et à la gravité, mais nous recommandons une certaine souplesse quant à la fréquence. Étant donné que les essais doivent tenir compte d'une variété de menaces, de dangers et d'événements à risque opérationnel, tous graves mais plausibles, ils doivent aussi reconnaître que ces événements n'entraîneront pas tous le même niveau de risque. Dans ces cas-là, des tests moins fréquents qu'une fois par an peuvent être adéquats.

3.2.1 L'énoncé de la propension à prendre des risques opérationnels expose clairement les types de risques et fixe des limites d'acceptation du risque quantifiables

Nous trouvons inhabituel que la définition de la propension à prendre des risques dans cette section fasse référence aux « activités courantes ». Veuillez consulter nos commentaires ci-dessus à la section 2.2.1. Cela ne correspond pas aux pratiques généralement acceptées.

3.3.1.1 Des outils sont employés pour établir le profil de risque de l'IFF

Bien que nous reconnaissions que les outils identifiés sont couramment utilisés, fournir une liste et inclure des descriptions détaillées est normatif. Nous recommandons de modifier le libellé pour préciser que ces outils ne sont que des exemples et que l'IFF devrait déterminer les outils appropriés à la nature des risques opérationnels examinés et évalués.

Bien que nous soyons heureux de lire l'énoncé suivant « la taille et de la nature de l'IFF, de la complexité de ses activités, de sa stratégie, de son profil de risque et de l'environnement de risque pour déterminer les outils qu'il convient d'employer », l'inclusion de détails relatifs aux outils suggère qu'ils sont obligatoires. Ce niveau de détail devrait être inclus dans une annexe à titre d'exemples d'outils.

4. Domaines liés à la gestion du risque opérationnel qui renforcent la résilience opérationnelle

Nous recommandons que la liste des domaines soit décrite comme « incluant, mais sans s'y limiter », car la liste fournie n'est pas exhaustive.

4.1.3 Mise à l'essai des plans de continuité des activités

Dans cette section, nous notons qu'il est fait mention de « diverses circonstances défavorables ». Cela devrait-il être « défavorable mais plausible »? Une définition des « circonstances défavorables » peut également s'avérer utile. Comme indiqué précédemment, il serait également utile de mettre à jour la ligne directrice E-18 afin de saisir les types de scénarios.

4.4 Gestion du changement

Dans la liste à puces de cette section, on peut lire : « tenir compte des risques liés aux

ressources humaines, à la gestion du risque et aux technologies ». Le BSIF peut-il préciser ce qu'il entend par risques liés à la gestion du risque? En outre, nous aimerions comprendre pourquoi certaines catégories de risque opérationnel sont incluses et pas d'autres. Nous recommandons que la formulation soit modifiée comme suit « tenir compte des risques liés aux diverses catégories de risque opérationnel ».

Nous recommandons également de modifier la mention « instaurer un changement important ». Il n'est pas nécessairement vrai qu'un changement important ait un impact sur les activités essentielles. L'accent devrait être mis sur les effets du changement sur les activités, les fonctions et les activités essentielles jugées à risque plus élevé. Le changement peut être important ou non, mais s'il a une incidence sur un processus essentiel, il serait prudent de faire preuve d'une diligence raisonnable renforcée.

4.7 Gestion du risque lié aux données

Nous convenons que la gestion du risque lié aux données est importante. Les lois fédérales et provinciales sur la protection des renseignements personnels décrivent les attentes en détail. Nous recommandons d'inclure une référence à la législation sur la protection des renseignements personnels afin d'éviter les dédoublements et les attentes contradictoires.

Nous nous interrogeons sur la nécessité d'une propension distincte à prendre des risques en ce qui concerne le risque lié aux données, au lieu de le gérer en fonction des tolérances au risque opérationnel. La prise en compte des données, notamment leur type, leur nature et leur utilisation, devrait contribuer à d'autres évaluations de risques.

L'ICA vous est reconnaissant de lui avoir donné la possibilité de formuler des commentaires sur ces questions et il serait heureux d'en discuter avec vous pendant tout le processus.

Veuillez transmettre vos questions à Chris Fievoli, FICA, actuaire, communications et affaires publiques, au 613-236-8196, poste 119 ou par courriel à chris.fievoli@cia-ica.ca.

Veuillez agréer l'expression de mes sentiments les meilleurs.

Le président de l'Institut canadien des actuaires,
Steve Prince, FICA

L'Institut canadien des actuaires (ICA) est l'organisme de qualification et de gouvernance de la profession actuarielle au Canada. Nous élaborons et maintenons des normes rigoureuses, partageons notre expertise en gestion du risque et faisons progresser la science actuarielle pour améliorer la vie des gens au Canada et à l'échelle du monde. Nos plus de 6 000 membres utilisent leurs connaissances en mathématiques, en statistiques, en analyse de données et en affaires dans le but de prodiguer des services et des conseils de la plus haute qualité afin d'aider les personnes et les organisations canadiennes à faire face à leur avenir en toute confiance.