Autorité
des marchés
financiers

Décembre 2024

# Bilan du sondage portant sur la résilience opérationnelle des institutions financières

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2024
ISBN 978-2-550-99131-1

# Table des matières


**Préambule** **5**

**Introduction** **6**

Thème 1 - La résilience opérationnelle 10
Thème 2 - La gouvernance 12
Thème 3 - Les services commerciaux importants 14
Thème 4 – La continuité des activités et la gestion des tiers 16

**Conclusion** **18**

**Annexe** **21**
Les résultats détaillés 22

# Préambule

L'Autorité des marchés financiers (l'AMF) a à cœur de favoriser la résilience du système financier québécois et de ses parties prenantes, qui font face à des enjeux émergents et opèrent dans des conditions toujours changeantes.

Au cours des dernières années, l'AMF a entrepris un dialogue avec les institutions financières dans un objectif de sensibilisation et de partage d'information sur les pratiques contribuant au rehaussement de la résilience opérationnelle. À ce titre, un colloque virtuel tenu en février 2023 a permis d'entendre l'avis d'institutions financières innovantes sur le choix, la mise en place et la mise à l'essai de pratiques clés de résilience opérationnelle leur permettant de gérer les perturbations affectant leurs activités essentielles.

À la suite de ce colloque et suivant l'objectif de maintenir le dialogue ouvert, l'AMF a transmis à l'automne 2023, à toutes les institutions financières autorisées opérant au Québec, le *Sondage sur les bonnes pratiques de résilience opérationnelle*. Le but de cet exercice était de brosser un portrait de l'état actuel des pratiques de résilience opérationnelle adoptées par les institutions opérant au Québec pour faire face aux nombreuses perturbations.

Ce sondage a couvert une variété de thèmes qui contribuent directement au rehaussement de la résilience opérationnelle, tels que l'identification des services commerciaux importants, la tolérance aux perturbations, la continuité des activités et la gestion des tierces parties.

Les résultats du sondage permettront à l'AMF d'identifier et de prioriser les travaux de rehaussement des encadrements existants selon les normes observées au niveau international, conjointement avec l'industrie, suivant l'objectif d'optimiser la charge de conformité. De plus, le sondage permettra aux institutions de comparer leurs initiatives de résilience opérationnelle à celles de leurs pairs.

Ce rapport présente une compilation anonymisée des pratiques de résilience opérationnelle au sein des institutions financières, quelques constats à l'égard de ces pratiques ainsi que certains des commentaires formulés par les institutions lors de cet exercice de sensibilisation.

L'AMF remercie les institutions de leur généreuse participation à cet exercice et espère que les résultats sauront les inspirer dans l'élaboration et le déploiement de leurs stratégies de résilience opérationnelle.

# Introduction

Dans le cadre de cet exercice de sensibilisation, l'AMF a développé un questionnaire sur les principaux thèmes introduits dans la réglementation émise par des régulateurs étrangers à l'égard de la résilience opérationnelle au cours des dernières années.

L'exercice s'est déroulé du 25 septembre au 10 novembre 2023 auprès de l'ensemble des institutions financières autorisées opérant au Québec. Les résultats ont été compilés à partir des réponses données dans les 254 questionnaires reçus par l'AMF.

# Quatre grands thèmes abordés

## Thème 1
## La résilience opérationnelle

L'objectif de ce premier thème était de mettre en perspective dans quelle mesure le concept de résilience opérationnelle se distingue de celui de la résilience organisationnelle et de la continuité des activités dans les opérations courantes des institutions et de comprendre l'importance accordée à ce concept par rapport aux autres priorités d'entreprise. Ce thème visait aussi à identifier la portée des initiatives de résilience opérationnelle déployées et les difficultés rencontrées lors de leur déploiement.

## Thème 2
## La gouvernance

Ce thème visait à connaître la planification, le développement et la mise en œuvre des objectifs et stratégies de résilience opérationnelle, l'évaluation de leur efficacité ainsi que le partage et l'assignation des rôles et responsabilités. Les investissements consacrés à ces initiatives ont également été abordés.

## Thème 3
## Les services commerciaux importants, leur conception et leur cartographie

Ce thème visait à fournir un éclairage sur la façon dont les institutions déterminent quels sont les services commerciaux importants dans leur organisation et dans quelle mesure ils ont été dûment identifiés. En outre, ce thème visait à connaître la façon dont les institutions s'assurent de l'exhaustivité de l'identification des services commerciaux importants et de la documentation de toutes les ressources requises et de leur interdépendance.

## Thème 4
## La continuité des activités et la gestion des tiers

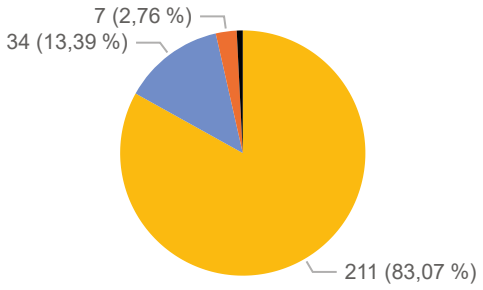
L'objectif de ce thème était d'identifier les plans en place pour faire face aux perturbations opérationnelles et comprendre les approches et stratégies de test établies notamment par le biais d'une cartographie des services commerciaux importants ou de la collaboration avec les tierces parties critiques.

# Distribution des répondants

## Répondants selon les lois appliquées

**Légende**

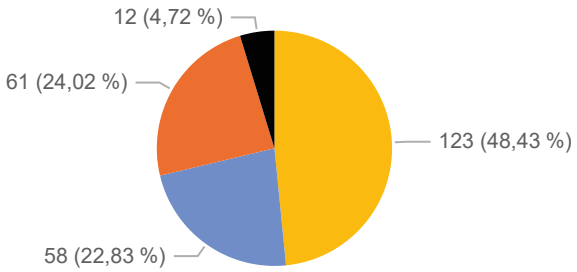
- Loi sur les assurances (LA)
- Loi sur les sociétés de fiducie et les sociétés d'épargne (LSFSE)
- Loi sur l'Assurance-dépôt (LAD)
- Loi sur la distribution de produits et services financiers (LDPSF)




## Répondants selon la charte

**Légende**

- Charte du Canada
- Charte du Québec
- Charte d'un État ou pays étranger
- Charte d'une autre province ou d'un territoire du Canada



# Thème 1
# La résilience opérationnelle

**Parmi les questions soumises aux institutions financières :**

- Comment définissez-vous la résilience opérationnelle?
- Comment distinguez-vous la résilience opérationnelle de la continuité des activités dans votre institution?
- Y a-t-il une distinction entre la résilience opérationnelle et la résilience organisationnelle dans votre institution?
- Par rapport à d'autres priorités d'entreprise/ stratégiques quelle importance a la résilience opérationnelle au sein de votre institution?
- Votre institution a-t-elle un programme ou un projet de résilience opérationnelle?

**Quelques constats dégagés des réponses reçues**

La gamme de définitions de la résilience opérationnelle est très variée et inspirée dans certains cas de celles proposées par les organismes de normalisation ou d'autres régulateurs, comme ceux du Royaume-Uni ou des États-Unis.

La résilience opérationnelle est comprise comme étant un complément à la continuité des activités, la gestion des risques et plus particulièrement les risques opérationnels.

Elle est aussi comprise comme une introduction de nouveaux concepts ou simplement un chevauchement avec les activités de la continuité des activités.

La majorité des institutions ont un programme de résilience opérationnelle en place. Celles qui n'ont pas intégré les éléments clés menant à la résilience de leurs opérations sont conscientes de leur « retard » et du fait qu'elles devront voir à cette mise en œuvre.

Pour ce faire, elles capitalisent sur les précisions à venir dans les encadrements, moment où elles ont l'intention d'intensifier les efforts.

Les difficultés rencontrées par les institutions financières pour mettre en œuvre un programme de résilience opérationnelle sont principalement attribuables aux contraintes liées à la compétence, aux connaissances, à la formation et à l'expérience nécessaires des ressources.

**Extraits des commentaires reçus des institutions financières**

*« La résilience opérationnelle est une priorité absolue, car elle améliorera notre capacité à résister et à nous rétablir suivant des événements perturbateurs et à maintenir la confiance de nos clients. (…) avec de solides mesures de résilience opérationnelle, nous pouvons minimiser les temps d'arrêt, atténuer les risques et maintenir nos opérations dans des situations défavorables. (…) La résilience opérationnelle contribue à préserver notre réputation et les intérêts de nos clients et parties prenantes. »*

*« Nous continuons d'investir dans la mise en œuvre d'un programme de résilience opérationnelle (…) il faudra un certain temps à l'organisation pour gagner en maturité et connaître le changement de culture et de mentalité nécessaire pour améliorer notre résilience. »*

*« Un certain manque de sensibilisation et de compréhension de la résilience opérationnelle au sein de l'organisation rend difficile l'établissement de priorités (…) L'évolution du paysage réglementaire pose des défis d'interprétation dans la construction de programmes. »*

# Thème 2
# La gouvernance

**Parmi les questions soumises aux institutions financières :**

- Que pensez-vous d'une nomination au niveau du conseil d'administration chargée d'évaluer la résilience à tous les niveaux et de veiller à ce que tous les efforts de renforcement de la résilience au sein de l'institution soient alignés et coordonnés?
- Comment vous assurez-vous que le conseil d'administration et la haute direction assurent une surveillance et une remise en question efficaces?
- Comment évaluez-vous l'efficacité de votre structure de gouvernance de la résilience opérationnelle?
- Quel niveau de connaissances et de compétences existe au niveau de la haute direction pour la résilience opérationnelle?

**Quelques constats dégagés des réponses reçues**

- Les avis convergent quant à la non-nécessité qu'un membre du conseil d'administration soit spécifiquement chargé d'évaluer le niveau de maturité de l'institution à l'égard de la résilience opérationnelle.
- Il est ressorti que les cadres supérieurs, y compris les membres du conseil d'administration, ont une compréhension adéquate, parfois même spécialisée, permettant d'assurer la supervision de la mise en œuvre d'un modèle d'exploitation résilient.
  - — Certaines institutions estiment toutefois que davantage de formations et d'ateliers, y compris des exercices de table, seraient utiles pour déterminer avec plus de précision les rôles et responsabilités des parties prenantes au sein de l'institution.
- La plupart des institutions indiquent qu'une structure de gouvernance documentée est en place et que les rôles et responsabilités de la haute direction ont été définis pour la mise en œuvre d'une approche de résilience opérationnelle efficace.

**Extraits des commentaires reçus des institutions financières**

- *« La résilience opérationnelle est actuellement en cours de développement. La structure de gouvernance sera alignée sur les objectifs de résilience stratégique et opérationnelle de l'organisation. »*
- *« On estime que ce qui est important, c'est que les membres du conseil d'administration possèdent les compétences, les connaissances et l'expérience requises dans les domaines de gestion des risques couvrant la technologie, la cybersécurité, les tiers et les interruptions d'activité afin d'assurer la surveillance requise de la résilience opérationnelle. »*
- *« Un membre du conseil d'administration s'est vu confier la responsabilité du programme de résilience opérationnelle, avec des dispositions de gouvernance en place pour assurer la surveillance des cadres de risque plus larges/connexes. »*
- *« La direction, et non les membres du conseil d'administration, devrait être responsable de l'évaluation de la résilience à tous les niveaux et de la garantie que tous les efforts sont alignés et coordonnés. Le conseil d'administration devrait fournir une remise en question constructive et une surveillance de ces activités comme il le fait pour d'autres activités commerciales. »*

# Thème 3
# Les services commerciaux importants

**Parmi les questions soumises aux institutions financières :**

- Votre institution financière a-t-elle identifié et documenté des services commerciaux importants qui, s'ils étaient interrompus, pourraient nuire aux consommateurs ou à l'intégrité du marché?
- Dans quelle mesure avez-vous complété l'inventaire de vos services commerciaux importants et de ses interdépendances?
- À quelle fréquence testez-vous vos capacités de réponse et de récupération pour différents scénarios perturbateurs?
- Comment comptez-vous utiliser la cartographie des services commerciaux importants dans votre approche de test?

**Quelques constats dégagés des réponses reçues**

- La mise en place d'une structure de gouvernance pour l'identification des services commerciaux importants est souvent présente.
  - — L'interprétation de ce que constitue concrètement un service commercial important varie, tout comme la complétion de l'exercice.
  - — La distinction entre les concepts d'activité critique et de service commercial important est souvent difficile à établir.
- Les exigences de résilience pour les services commerciaux importants et leurs interdépendances sont fréquemment documentées et tenues à jour en consolidant le tout en une liste unique pour en assurer l'intégrité.
  - — Cette liste fait dans certains cas l'objet d'un examen indépendant.
- Il y a une bonne compréhension des données de cartographie des services commerciaux importants.
  - — L'inclusion de ces données dans des approches de test est envisagée et cela pourrait même être étendu aux tierces parties critiques.

**Extraits des commentaires reçus des institutions financières**

- *« Nous avons réalisé plusieurs évaluations pilotes de la résilience opérationnelle de services commerciaux importants identifiés au sein de plusieurs de nos secteurs d'activités. Les enseignements tirés de ces projets pilotes ont été intégrés et, par conséquent, nous élaborons actuellement un programme de résilience opérationnelle des entreprises, ainsi qu'une feuille de route globale du programme. »*
- *« (…) l'intention de développer une stratégie de résilience opérationnelle, en effectuant une analyse des lacunes des systèmes commerciaux importants (…) prioriser les services commerciaux critiques (…) améliorer l'efficacité de notre système de gestion de la continuité des activités. »*
- *« (…) reconnaît l'importance de renforcer l'appropriation au sein de l'organisation et de développer des stratégies de résilience, y compris la résilience des tiers. »*
- *« Nous exploitons l'importante cartographie des services métiers dans le développement et l'exécution de nos exercices de scénarios de perturbations graves mais plausibles. Nous continuerons à étendre nos exercices pour les rendre plus complexes et refléter les perturbations émergentes. »*

# Thème 4
# La continuité des activités et la gestion des tiers

**Parmi les questions soumises aux institutions financières :**

- En cas de perturbation opérationnelle, comment préparez-vous et priorisez-vous vos ressources et actions afin d'assurer la continuité de vos services commerciaux et de minimiser les dommages aux consommateurs/clients?
- Avez-vous une liste de l'ensemble des services fournis par des tiers et leurs fournisseurs au sein de votre institution?
- Quels problèmes de tiers ou d'externalisation votre institution financière a-t-elle rencontrés, le cas échéant?
- Comment identifiez-vous votre dépendance vis-à-vis des services fournis par des tiers (y compris les intra-affiliés) pour la fourniture de services commerciaux importants qui pourraient entraîner un préjudice pour le client?

**Quelques constats dégagés des réponses reçues**

- Les institutions ont un cadre de continuité formel en place et une approche de test des plans de continuité bien définie

  — Leur capacité de réponse et de récupération à différents scénarios perturbateurs est testée sur une base annuelle.

  — Les plans de récupération tiennent compte des services fournis par des tiers.

- Les problèmes rencontrés avec les tiers portent essentiellement sur la sécurité des données, les problèmes informatiques et les interruptions de services.

  — La majorité des institutions effectue périodiquement une diligence raisonnable sur des tiers nouveaux et existants pour évaluer et gérer les risques et vulnérabilités qui sont susceptibles d'être introduits dans l'environnement d'exploitation.

- Les institutions procèdent à des examens indépendants périodiques de leurs processus et contrôles et transmettent les résultats des tierces parties à la haute direction ou au conseil d'administration.

  — Leurs registres des tiers sont mis à jour périodiquement et sont de plus examinés de manière indépendante.

**Extraits des commentaires reçus des institutions financières**

- *« La priorisation s'effectue en fonction de la criticité et des exigences de résilience propres aux activités critiques ou aux systèmes informatiques, en fonction du scénario considéré. Les équipes de sécurité disposent d'une visibilité et de rapports provenant de plusieurs sources afin de répondre de manière proactive aux interruptions de toute nature. »*

- *« Nous disposons de programmes éprouvés de gestion des risques liés aux tiers et de gestion de la continuité des activités, et sommes en train de faire évoluer les programmes existants afin d'intégrer plus explicitement les exercices de test pour les services commerciaux importants. »*

- *« Un processus formel d'analyse post-incident est en place, avec des analyses axées sur les pannes graves (…) L'analyse prend en compte à la fois les données collectées pendant et après l'incident. Les leçons apprises sont intégrées aux processus opérationnels appropriés. »*

- *« L'identification du risque de concentration est en place depuis 10 ans (…) Bien que les services commerciaux importants aient été identifiés et les dépendances envers les tiers cartographiées, ceux-ci ne figurent pas actuellement dans notre registre des risques envers les tiers. »*

# Conclusion

***« La résilience est devenue incontournable dans un monde où les perturbations se multiplient. Il est temps d'agir. Nous devons passer des paroles aux actes. Le moment présent doit être considéré comme une opportunité de construire (…) un nouveau modèle de leadership pour l'avenir. Pour ce faire, les organisations doivent reconnaître où elles se situent dans leur parcours de résilience et les dirigeants ont besoin d'occasions de partager leurs expériences, d'apprendre des meilleures pratiques et de nouer des partenariats pour élaborer des solutions communes. »***

*World Economic Forum Resilience Consortium*

L'Organisation internationale de normalisation (ISO), une fédération mondiale d'organismes nationaux de normalisation, a défini la résilience organisationnelle comme étant la capacité d'une organisation à absorber et à s'adapter dans un environnement changeant pour lui permettre d'atteindre ses objectifs, de survivre et de prospérer.

Selon l'ISO, cette résilience organisationnelle est soutenue par plusieurs disciplines de gestion et stratégies, dont celles qui sont généralement abordées sous le thème de la résilience opérationnelle à travers le monde (…), notamment la gestion de la continuité des activités et la gestion de la sécurité de l'information et de la cybersécurité.

La résilience opérationnelle est une préoccupation croissante dans le secteur des services financiers. Face aux conséquences réelles et potentielles de plusieurs perturbations opérationnelles, des initiatives réglementaires se sont développées rapidement à travers le monde, suivant l'objectif de répondre aux défis croissants des institutions financières à l'égard de leurs dépendances à la technologie, à l'interconnexion et à l'évolution des menaces.

Le contrôle des relations avec les tiers et la gestion des risques associés se sont notamment intensifiés, reflétant les inquiétudes concernant la concentration et d'autres risques associés à l'externalisation de fonctions critiques à des entités potentiellement non réglementées.

Les perturbations opérationnelles ont des conséquences importantes sur les institutions financières et sur les consommateurs de produits et services financiers. Selon les institutions ayant participé au sondage, ces perturbations proviennent notamment d'un nombre croissant de pannes technologiques, de cyberattaques, d'événements climatiques et parfois même d'une combinaison simultanée de différents facteurs.

Il ressort des résultats que les institutions sont conscientes des conséquences de l'accroissement de ces perturbations, malgré qu'elles rapportent avoir, à ce jour, subi des conséquences limitées face aux perturbations des dernières années.

***« La résilience est la capacité à faire face à l'adversité, à résister aux chocs et à s'adapter et accélérer en permanence lorsque des perturbations et des crises surviennent au fil du temps. »***

*World Economic Forum Resilience Consortium*

Les résultats du sondage démontrent que les institutions financières sont en voie de déployer des initiatives de résilience opérationnelle, mais qu'elles se trouvent à des degrés de maturité variés. Qu'il s'agisse de la définition même de ce concept, des rôles et responsabilités attribués au sein des organisations, des travaux mis en œuvre pour identifier les services commerciaux importants ou encore de la considération des impacts des perturbations sur l'institution et sa clientèle, les changements de culture s'opèrent différemment.

Les réponses recueillies confirment le besoin pour l'AMF de bonifier certains de ses encadrements afin d'appuyer les institutions financières dans leur transition vers un modèle d'affaires plus résilient.

Les résultats du sondage ont mis en lumière un besoin d'harmoniser les pratiques au sein des institutions. L'AMF pourrait répondre à ce besoin en arrimant son encadrement prudentiel aux nouvelles normes internationales établies sur la résilience opérationnelle, comme l'ont recommandé les institutions elles-mêmes.

***« Un élément différenciateur clé est l'optique des opérations critiques, en conjonction avec la vision de bout en bout, l'accent mis sur l'impact, l'utilisation de la tolérance aux perturbations pour orienter les décisions sur les investissements en matière de résilience et la prise en compte de la résilience des tiers. »***

*Banque des règlements internationaux*

La collaboration des institutions participantes à ce sondage a également permis d'identifier plusieurs de leurs besoins visant à rehausser leur résilience opérationnelle.

Reconnaissant d'emblée l'importance des risques de la résilience opérationnelle et son caractère systémique, l'AMF analysera les différentes avenues qui s'offrent à elle en vue de soutenir l'industrie.

Les différents constats qui se dégagent permettront à l'AMF de poursuivre les discussions avec les institutions financières, notamment quant à l'opportunité de les doter d'encadrements adéquats et contemporains visant les différentes facettes de la résilience opérationnelle et la saine gestion des risques sous-jacents.

# Annexe

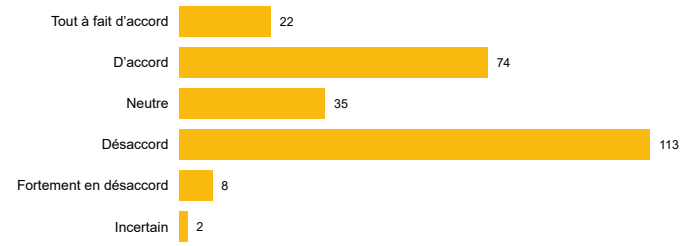
# Les résultats détaillés

La présente annexe présente, de manière détaillée et anonymisée, les réponses données dans les 254 questionnaires reçus par l'AMF, pour chacune des questions qui a fait l'objet de l'exercice de sensibilisation.

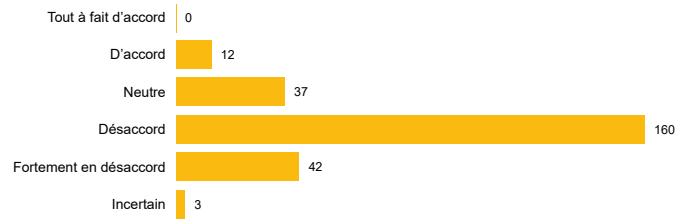
Sont également présentés, pour chaque thème, différents commentaires ou observations généreusement fournis par les institutions participantes.

## **Q100-2** Comment distinguez-vous la résilience opérationnelle de la continuité des activités dans votre institution?

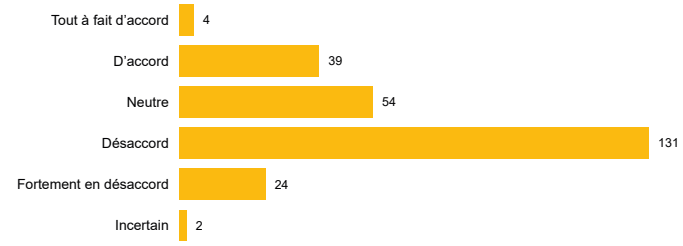
Continuité des Activités et Résilience Opérationnelle sont considérées comme des fonctions différentes avec des objectifs différents dans notre organisation



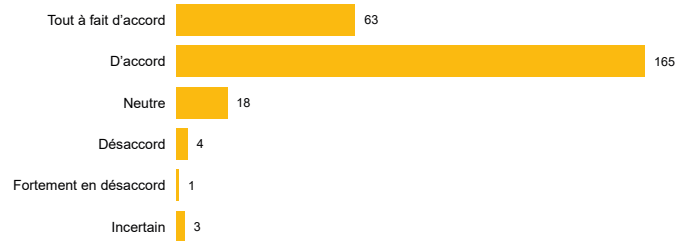

Continuité des Activités a été rebaptisée Résilience Opérationnelle dans notre organisation, mais aucun changement n'a été apporté aux responsabilités professionnelles



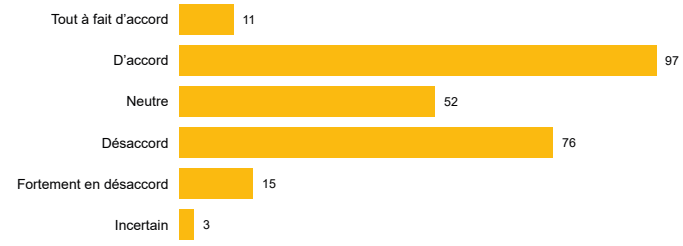

Continuité des Activités et Résilience Opérationnelle sont synonymes dans notre organisation



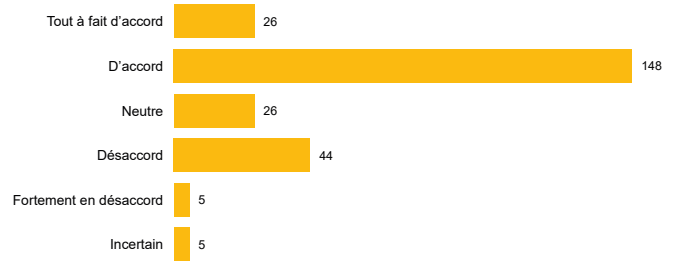

Continuité des Activités fait partie de Résilience Opérationnelle, il soutient la résilience




Il y a un chevauchement entre Continuité des Activités et Résilience Opérationnelle, mais nous n'avons pas clairement défini les différences




Continuité des Activités est un outil/processus pour piloter Résilience Opérationnelle




**Certains des commentaires formulés par les institutions :**

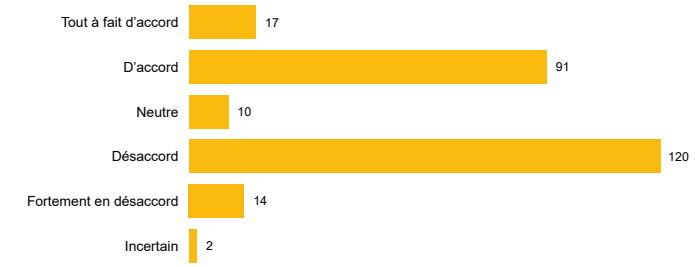
*« La continuité des activités et la résilience opérationnelle sont deux équipes distinctes qui collaborent sur une base régulière et qui partagent des objectifs communs. »*

*« La résilience opérationnelle est aussi un état d'esprit qui s'attache à tout ce qu'ils font en matière de gestion de crise, de perturbation des activités, de gestion des risques liés aux tiers, de risque lié aux voyages, de préparation à une pandémie, etc. »*

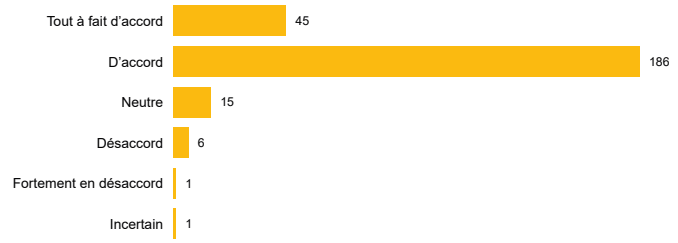
*« L'objectif à long terme du renforcement de la résilience opérationnelle est de protéger la réputation et la viabilité à long terme d'une organisation, tandis que l'objectif de la gestion de la continuité des activités est de minimiser l'impact potentiel d'un événement perturbateur. »*

# **Q100-3** Dans quelle mesure êtes-vous en accord avec les énoncés suivants?

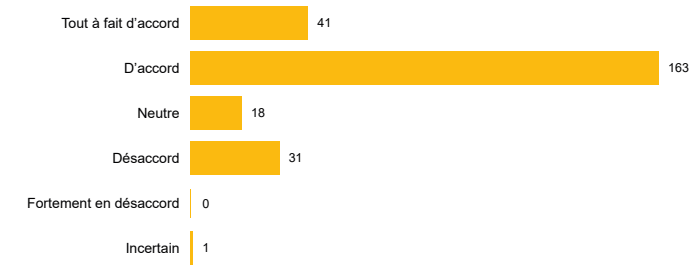
Continuité des Activités est réactif et axé sur la réponse et le rétablissement



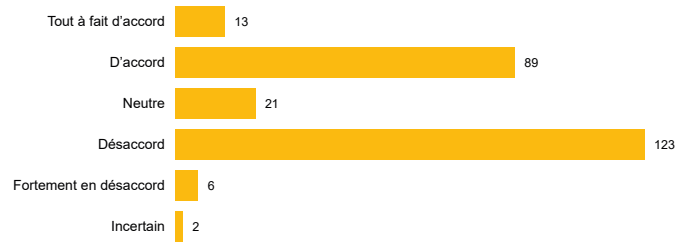

Résilience Opérationnelle est proactif; cela fonctionne pour prévenir les interruptions et fournir une capacité de récupération



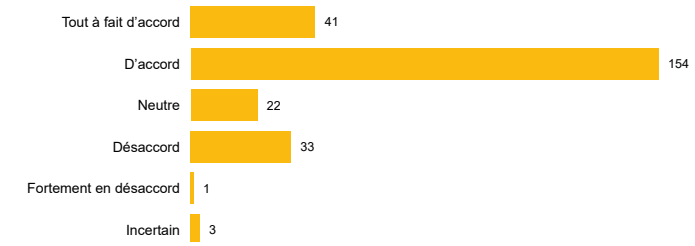

Continuité des Activités tient compte de la probabilité de perturbation



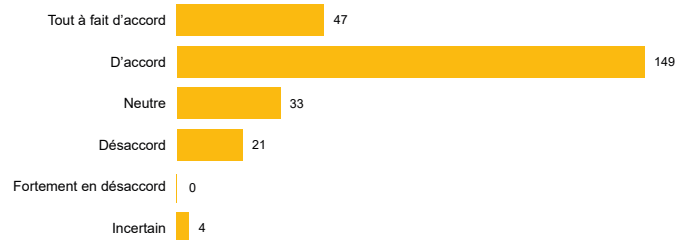

L'accent principal de Continuité des Activités est mis sur l'impact interne pour l'organisation, lorsqu'elle est confrontée à un événement perturbateur




Continuité des Activités se concentre également sur l'impact interne et externe sur l'organisation lorsqu'elle est confrontée à un événement perturbateur




Résilience Opérationnelle se concentre sur les conséquences pour le client et le marché, face à un événement perturbateur




**Certains des commentaires formulés par les institutions :**

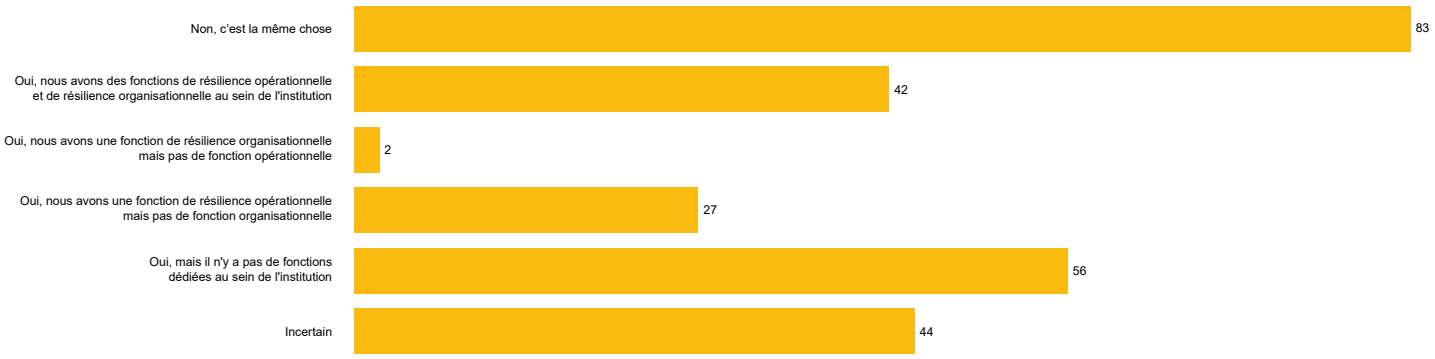
*« La résilience opérationnelle se concentre également sur les conséquences internes et externes lorsqu'elles sont confrontées à un événement perturbateur. Notre approche concernant les conséquences externes est centrée sur les clients et l'intégrité du marché. »*

*« Les impacts réputationnels, réglementaires, financiers et économiques qui touchent les partenaires et les clients sont pris en considération. »*

*« La résilience opérationnelle est une approche proactive qui implique l'identification des opérations critiques et la cartographie des dépendances internes et externes nécessaires pour les prendre en charge. (...) l'établissement de tolérances aux perturbations, la réalisation de tests de scénarios et l'établissement d'une culture qui favorise et renforce les comportements qui soutiennent la résilience opérationnelle et gère de manière proactive la culture et les risques de comportements qui peuvent influencer la résilience. »*

*« Le programme de résilience opérationnelle se concentre sur l'approche stratégique visant à maintenir les services commerciaux essentiels en cas d'événements extrêmes, mais plausibles qui pourraient avoir un impact non seulement sur l'institution, mais également sur ses clients et sur le marché financier en général. »*

## **Q100-4** Y a-t-il une distinction entre la résilience opérationnelle et la résilience organisationnelle dans votre institution




**Certains des commentaires formulés par les institutions :**

*« Nous ne définissons aucun de ces termes dans nos politiques et (…) pour l'instant, ces concepts ne se traduisent pas en fonctions dédiées dans notre organisation. Ces concepts restent donc vagues. »*

*« (…) la résilience organisationnelle rassemble la résilience financière et la résilience opérationnelle. Une entreprise peut être résiliente sur le plan opérationnel mais échouer néanmoins en raison de problèmes de liquidité et de capital, alors qu'une autre entreprise résiliente financièrement peut souffrir de problèmes opérationnels lui causant des dommages. La résilience opérationnelle fait référence à la capacité d'une organisation à résister et à s'adapter à diverses perturbations de processus, technologiques et/ou humaines. Il permet de garantir que les opérations commerciales critiques continuent de fonctionner malgré les perturbations, en atténuant les risques potentiels et en s'adaptant rapidement aux perturbations ou en s'en remettant rapidement. La résilience opérationnelle est essentielle pour que les organisations puissent bâtir et maintenir la confiance de leurs clients, protéger nos clients et nos marchés contre les dommages, et se conformer aux exigences réglementaires. »*

*« La résilience organisationnelle comprend tous les principaux domaines de l'entreprise : stratégique, capital/financier, technologique, opérationnel, culturel et d'apprentissage. La résilience opérationnelle se concentre principalement au niveau du modèle opérationnel - avec des contrôles, des politiques, une surveillance et des pratiques pour renforcer l'intégrité et la cohérence opérationnelles. »*

## **Q100-5** Par rapport à d'autres priorités d'entreprise/stratégiques quelle importance a la résilience opérationnelle au sein de votre institution?

**Certains des commentaires formulés par les institutions :**

*« La haute direction considère la résilience opérationnelle en tête de liste des priorités (…) liée à nos priorités stratégiques (…) élément fondamental de toutes les initiatives commerciales et stratégiques. »*

*« Après la pandémie de Covid-19 et dans un monde d'incertitude croissante, il est plus important que jamais de comprendre les risques pour l'organisation (…). »*

*« La résilience opérationnelle est une priorité absolue, car elle améliorera notre capacité à résister et à nous rétablir suite à des événements perturbateurs et à maintenir la confiance de nos clients. (…) contribue à préserver notre réputation et les intérêts de nos clients et parties prenantes. »*

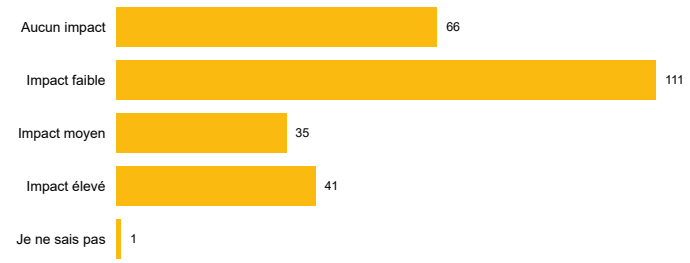
*« Ce concept est nouveau pour nous. La résilience opérationnelle apparait ainsi maintenant plutôt importante maintenant que nous y sommes sensibilisés! »*

*« La résilience opérationnelle est un aspect central de la stratégie informatique (Resilience by design). »*

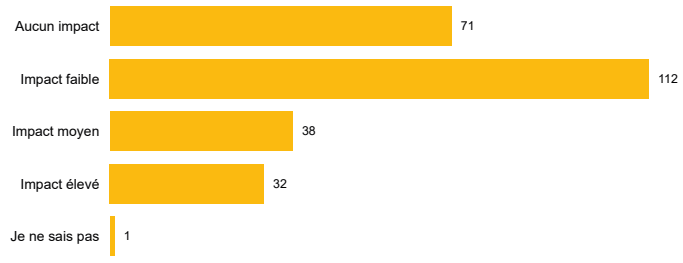
*« Nous commençons à travailler dans ce domaine et nous allons intensifier nos efforts à mesure que les directives réglementaires se précisent. »*

## **Q100-6** Hormis la pandémie, quel a été l'impact de la plus sévère perturbation opérationnelle subie au cours des dernières années sur les aspects suivants de vos activités?

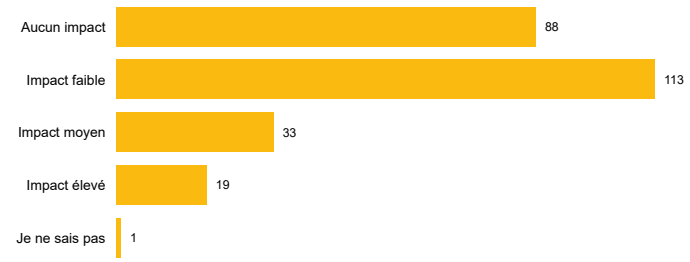
Impact Technologie



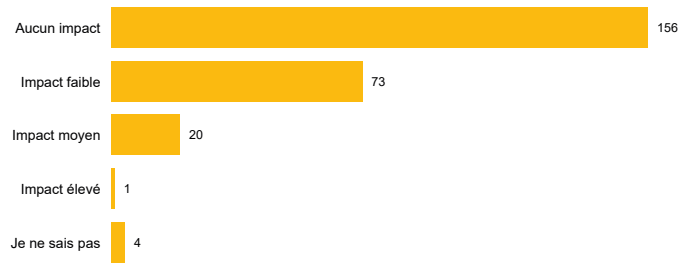

Impact Opérations (perturbation des processus/services essentiels…)



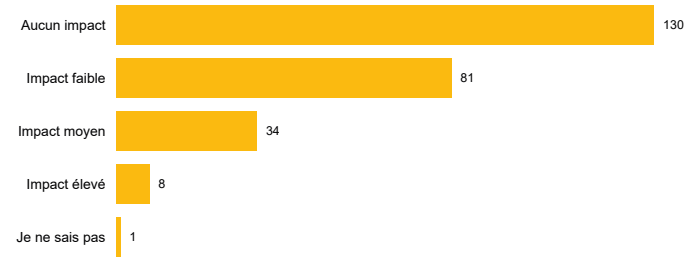

Impact Main d'œuvre



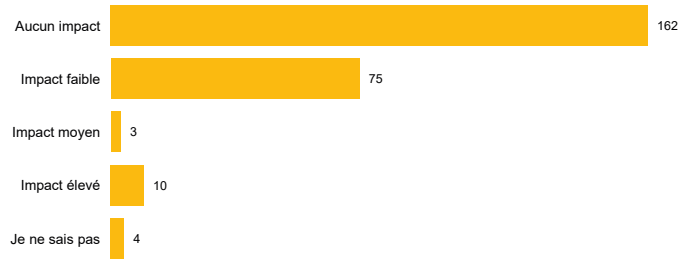

Impact Situation financière



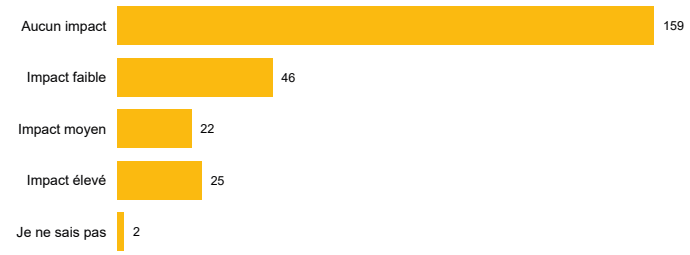

Impact Relations avec les clients et partenaires commerciaux




Impact Réputation/Solidité de la marque




Impact Stratégie d'entreprise




**Certains des commentaires formulés par les institutions :**

*« Nous avons connu plusieurs problèmes qui laissaient présager qu'une cyberattaque pourrait être en cours. Bien qu'il ne s'agisse pas d'un cyberincident, il s'agissait d'un bon "test" des protocoles de cybersécurité et de gestion de crise, avec l'occasion de tirer des leçons importantes. »*

*« Nous avons géré l'événement en suivant nos procédures de continuité des activités et avons encore amélioré notre redondance en recherchant et en mettant en œuvre des améliorations à partir des leçons apprises. »*

## **Q100-7** Par ordre d'importance, quels domaines (max. 3) ont présenté le plus de difficultés dans votre réponse à la perturbation la plus sévère subie au cours des dernières années (hormis la pandémie)?

| Énoncés | Priorité 1 | Priorité 2 | Priorité 3 | Total |
|---|---|---|---|---|
| Capacité à communiquer de façon efficace avec les parties prenantes internes | 14 | 14 | 7 | 35 |
| Capacité à collecter les informations appropriées rapidement et efficacement | 32 | 16 | 20 | 68 |
| Capacité à prendre des décisions en temps utile et en connaissance de cause | 2 | 7 | 5 | 14 |
| Clarté quant aux responsabilités de la réponse | 4 | 9 | 6 | 19 |
| Détermination des rôles et responsabilités et pouvoir de prise de décisions sur l'ensemble des équipes d'intervention | 8 | 7 | 6 | 21 |
| Capacité à utiliser les technologies/outils appropriées pour accroitre la capacité de la réponse | 18 | 20 | 25 | 63 |
| Capacité à hiérarchiser les actions, y compris la reprise et le rétablissement, selon le cas | 4 | 4 | 12 | 20 |
| Capacité de reconnaitre que l'incident constituait une crise et nécessitait par conséquent de remonter l'information et de mobiliser l'équipe dirigeante appropriée | 8 | 6 | 2 | 16 |
| Visibilité sur les incidences à l'échelle de toute l'organisation | 13 | 15 | 22 | 50 |
| Utilité du plan de réponse (ex. : gestion des crises, continuité de l'activité, reprise après sinistre, etc.) | 10 | 8 | 8 | 26 |
| Capacité à récupérer/rétablir les services et processus commerciaux essentiels aux opérations ordinaires | 35 | 12 | 5 | 52 |
| Capacité à maintenir les services et processus commerciaux critiques grâce à des mesures de continuité | 10 | 33 | 12 | 55 |
| Capacité à communiquer de façon efficace avec les parties prenantes externes | 1 | 23 | 15 | 39 |
| Capacité à influencer la couverture médiatique | 4 | 1 | 5 | 10 |
| Aucun domaine en particulier | 74 | 1 | 10 | 85 |

**Certains des commentaires formulés par les institutions :**

*« Engager continuellement les principales parties prenantes pour renforcer l'engagement, l'interconnectivité et améliorer les processus en cours d'exécution. Comprendre les impacts externes sur les fournisseurs à travers les événements est important et garantir une communication bidirectionnelle. »*

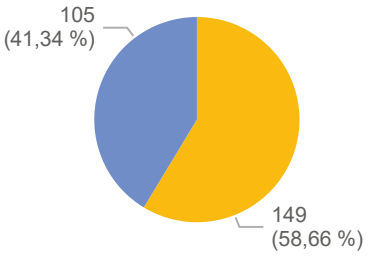
*« Dans le passé, les perturbations les plus notables étaient traitées rapidement et de manière transparente avec toutes les parties prenantes concernées afin d'éviter des impacts négatifs majeurs. (…) à mesure que les modèles commerciaux et opérationnels continuent d'évoluer, nous veillons à ce que les capacités, contrôles et protocoles de communication internes soient mis à jour et pertinents. »*

*« (…) communiquer et diriger des tiers est plus difficile en raison du manque de visibilité sur leurs opérations et leur résilience (…) capacité à recueillir des informations rapidement et efficacement a été entravée, car la perturbation faisait partie d'un incident tiers affectant plusieurs entités. Cela a à son tour entravé la capacité à communiquer efficacement avec les parties prenantes externes. »*

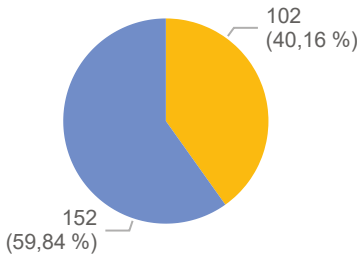
# **Q100-8** À quels types de perturbations craignez-vous que votre institution soit confrontée, ou continue d'être confrontée, sur les deux prochaines années?

**Légende** Oui Non

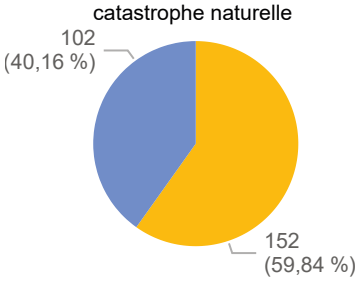
Aspects juridiques / réglementaires



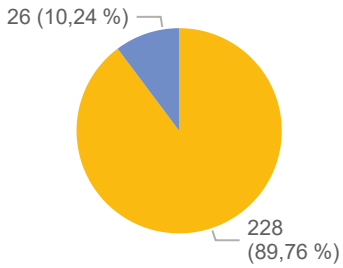

Pannes technologiques



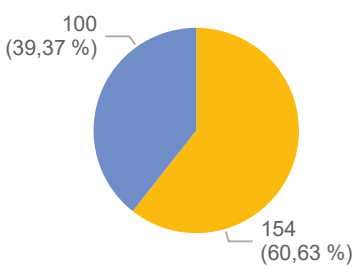

Changement climatique/ catastrophe naturelle



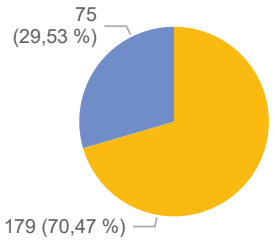

Vol de propriété intellectuelle



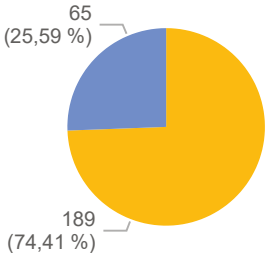

Recrutement employés / rotation dirigeant



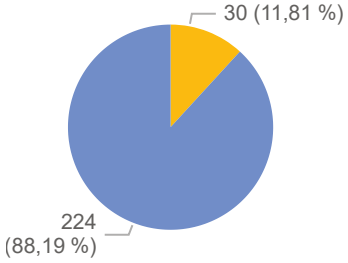

Géopolitique/Terrorisme/Sanitaire



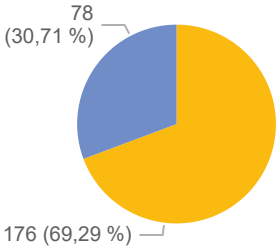

Pannes opérationnelles



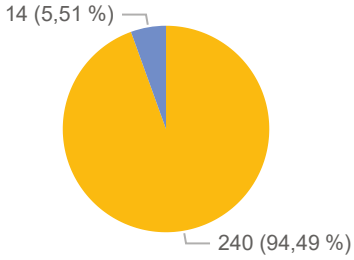

Cyberattaque



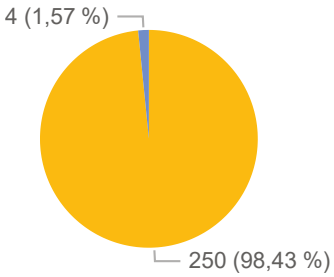

Pannes infrastructures essentielles



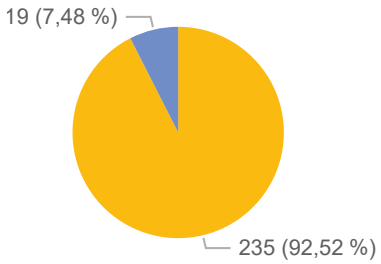

Comportement inapproprié de la main-d'oeuvre




Activisme des actionnaires




Aucune perturbation particulière



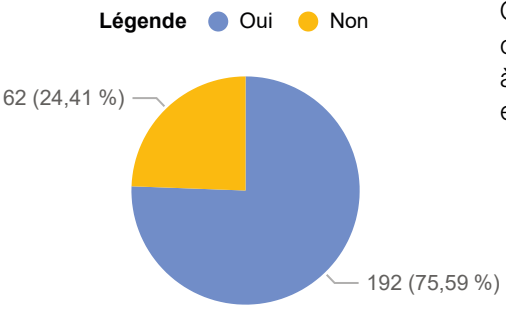

**Certains des commentaires formulés par les institutions :**

*« La panne d'un fournisseur critique/clé (chaîne logistique) ou la panne importante d'un tiers et également le risque de concentration avec les fournisseurs, l'infrastructure technologique. »*

*« La concurrence stratégique face au système bancaire ouvert, aux fintechs et aux changements réglementaires qui accompagneront ces forces en évolution. »*

*« Les exigences réglementaires supplémentaires à mesure que les normes et les modèles de gouvernance évoluent et nécessitent une surveillance et une réactivité accrues. »*

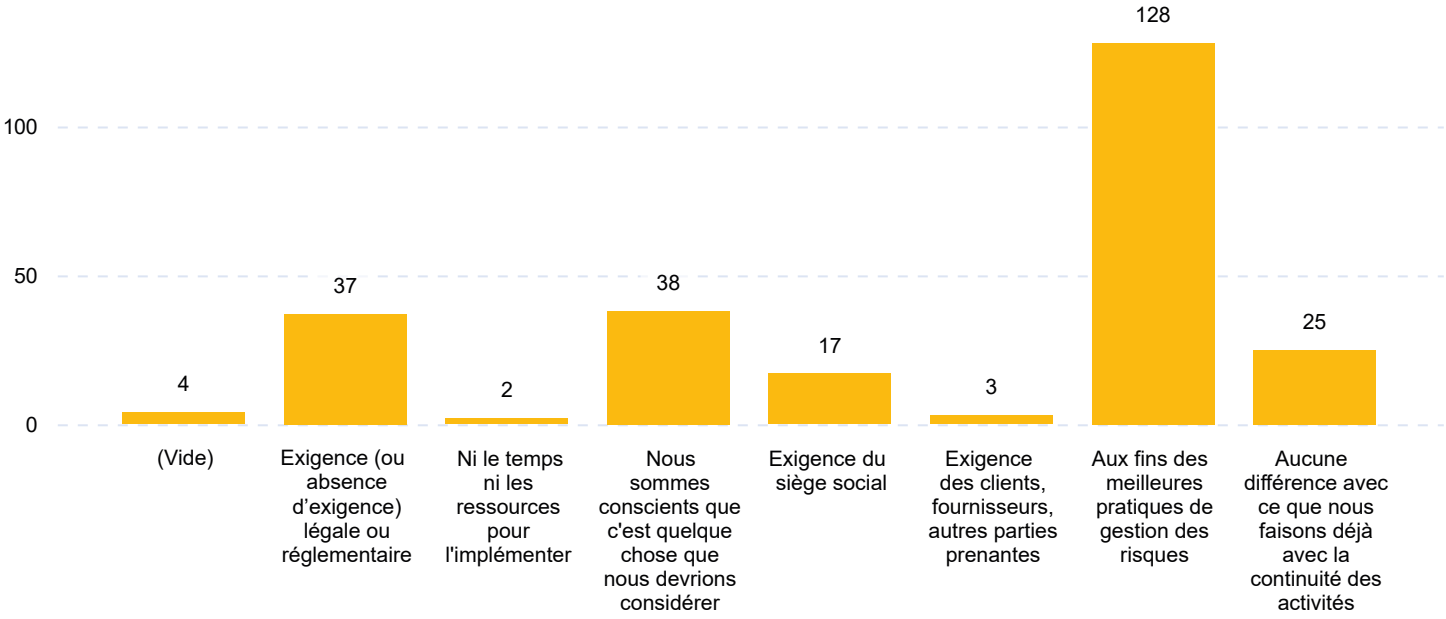
## **Q100-9** Votre institution a-t-elle un programme ou un projet de résilience opérationnelle?




Globalement, près de 76 % des institutions indiquent avoir en place un programme ou un projet de résilience opérationnelle. Ce taux est de 88 % pour les institutions à charte d'un État ou d'un pays étranger, 77 % pour celles à charte canadienne et 64 % pour celles à charte du Québec.

## **Q100-10** Expliquez la raison pour laquelle vous avez (ou n'avez pas) de programme ou projet de résilience opérationnelle.

**PARTIE A (Toutes les institutions)**




**Certains des commentaires formulés par les institutions :**

La majorité des institutions qui ont mis en place un programme ou projet de résilience opérationnelle l'ont fait prioritairement aux fins des meilleures pratiques de gestion. Elles ont aussi exprimé dans certains cas qu'il s'agissait d'une exigence de leur siège social ou d'une exigence réglementaire actuelle ou prochaine. Elles ont indiqué notamment que :

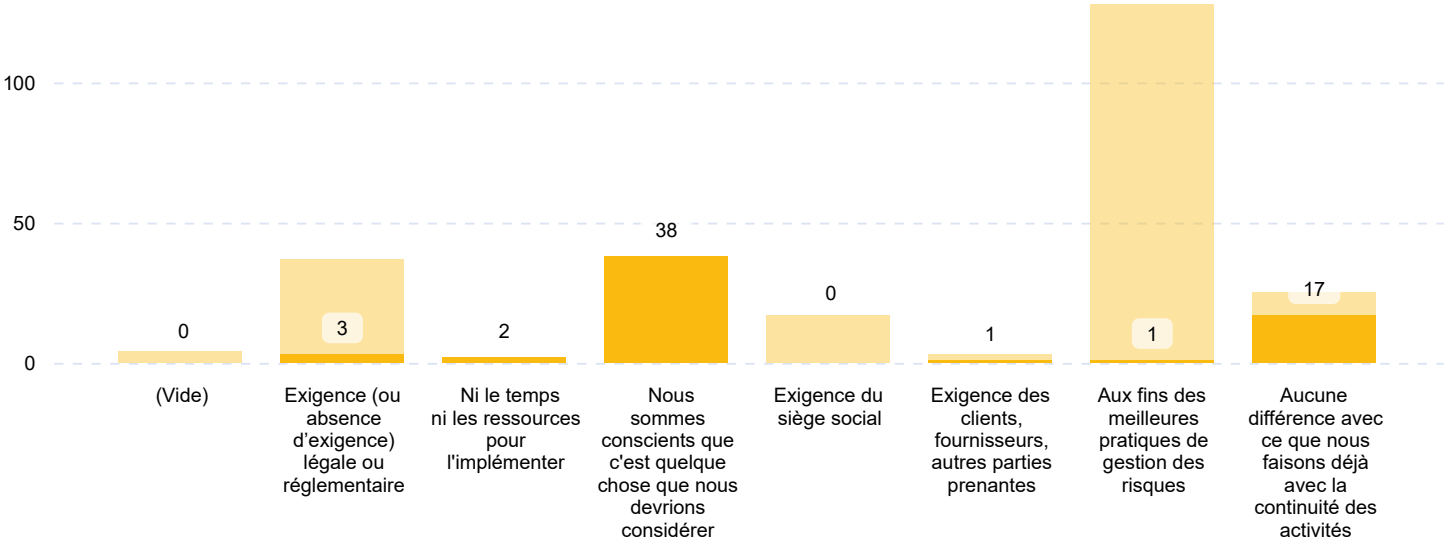
*« L'exercice est motivé par des exigences réglementaires, mais l'objectif du programme est de rendre l'organisation résiliente dès sa conception (« Resilience by design »). »*

*« Outre les exigences énoncées ci-dessus, l'organisation reconnaît l'importance d'un programme de résilience opérationnelle quelles que soient les exigences ou influences extérieures. »*

*« Le principal objectif est la gestion des risques, même si certains délais et livrables sont alignés sur les attentes réglementaires. »*

*« Nous sommes convaincus que le programme de résilience opérationnelle est bénéfique et répond aux attentes de nos clients, fournisseurs et parties prenantes. »*

**PARTIE B (Institutions n'ayant pas de programme)**




**Certains des commentaires formulés par les institutions :**

*« En cours d'élaboration d'un cadre pour intégrer diverses exigences réglementaires, notamment le risque lié aux tiers et le risque cybernétique et technologique. »*

*« Bien que nous n'ayons pas spécifiquement identifié de programme ou de projet de résilience, nous avons construit la résilience grâce à des changements organiques et aux leçons tirées des perturbations. »*

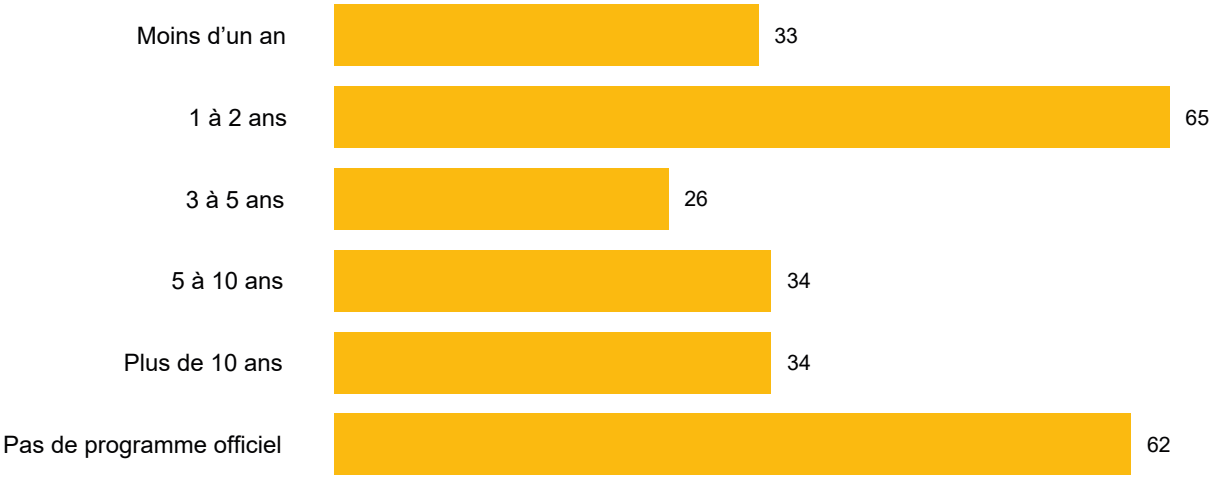
*« Nos programmes de continuité des activités et de reprise après sinistre ainsi que nos programmes couvrant la résilience technologique, la cyber-résilience, la résilience commerciale (gestion des risques d'entreprise) et la résilience des fournisseurs abordent et documentent de nombreux aspects de la résilience opérationnelle. »*

*« Nous en sommes aux premiers stades de la planification et attendons des conseils sur ce sujet (…). Pas de projet officiel pour l'instant. »*

*« Nous collaborons avec des pairs de notre secteur pour examiner les meilleures pratiques. La résilience opérationnelle est un sujet qui a commencé à gagner du terrain (…), une voie à suivre où nous intégrerons certains concepts dans notre programme existant. »*

*« Il s'agit d'un concept récent. Nous sommes une petite organisation (…), les ressources actuelles ne permettent pas d'entreprendre ce projet. »*

## **Q100-11** Depuis combien de temps votre programme de résilience opérationnelle existe-t-il?




**Certains des commentaires formulés par les institutions :**

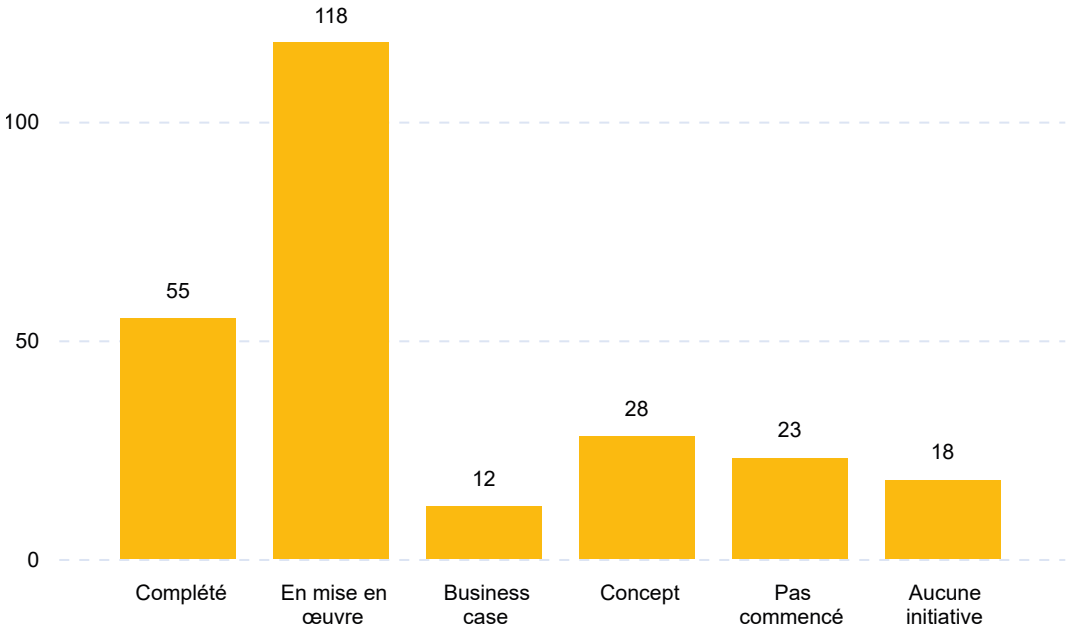
*« Nous intégrons activement les principes de résilience opérationnelle dans notre programme GRO depuis 2022. Cependant, des pratiques clés en matière de risque opérationnel liées à la résilience opérationnelle existent au sein de l'institution depuis plusieurs années. »*

*« Un programme formel de résilience opérationnelle a été créé il y a 2 ans pour relier les programmes de gestion des risques opérationnels et créer une capacité supplémentaire d'évaluation de la résilience. »*

*« Le programme dans un sens large a commencé, il y a plusieurs années, par un concept de «disaster recovery». Puis a évolué vers le concept de continuité des affaires, et finalement vers un concept de résilience opérationnelle, et ce, pour chaque secteur d'affaires. Le programme résilience opérationnelle (projet) a débuté à la fin 2020 pour la portion rançongiciel (phase conception et premier pas des correctifs en mode tactique). La portion relève a débuté plus vers la fin 2021. Depuis un an et demi, le programme (projet), consolidé et structuré sous le chapeau de la résilience opérationnelle, adresse l'ensemble des enjeux en mode tactique et stratégique afin de diminuer le risque de l'organisation. »*

*« Le programme a été rebaptisé Résilience opérationnelle au cours des dernières années, mais il existait auparavant sous le nom de Gestion de la continuité des activités et est en place depuis plus de 10 ans. »*

## **Q100-12** Où en est votre initiative ou projet sur la résilience opérationnelle?



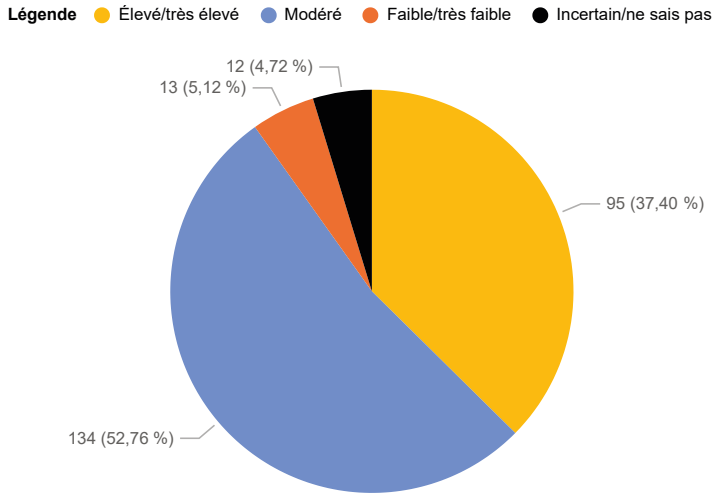

**Certains des commentaires formulés par les institutions :**

La majorité des institutions indique que leur projet de résilience opérationnelle est complété ou dans une phase de mise en œuvre. Elles indiquent notamment qu'elles sont en amélioration continue ou qu'elles mettent actuellement en œuvre un programme de résilience opérationnelle pluriannuel. Certaines institutions, à l'étape du concept, indiquent par ailleurs que :

*« Elles sont en train de revoir leurs exigences en matière de résilience opérationnelle pour déterminer les besoins et les exigences du programme. Cela se fera conformément aux lignes directrices et aux délais du BSIF E-21. »*

*« Nous réorientons notre attention vers les pratiques de continuité des activités et la conception de plans pour commencer à envisager une approche plus holistique de la résilience opérationnelle. »*

## **Q100-13** En pensant à l'approche globale, aux ressources et aux processus de votre institution, comment évaluez-vous sa capacité de résilience opérationnelle?




**Certains des commentaires formulés par les institutions :**

*« La résilience opérationnelle n'est pas un projet qui s'achève - c'est un programme en constante évolution et en maturation, intégrant les principes de continuité des activités dans toute l'organisation. »*

*« Organisation de petite taille = capacité de prendre en charge les processus rapidement. »*

*« La résilience opérationnelle est en mode « business as usual ». (...) résilience est une cible mouvante à mesure que notre paysage de menaces continue d'évoluer (...) nous nous concentrons sur l'amélioration continue et sur le fait de relever la barre de nos capacités de résilience. »*

*« Comme organisation, nous testons et raffinons constamment les processus à l'aide de diverses pratiques tel que des exercices sur table. »*

*« Le programme de résilience opérationnelle est un projet en mode construction ; la pleine capacité n'a pas encore été mise en œuvre. »*

*« Des évaluations pilotes de résilience opérationnelle de bout en bout ont été réalisées pour plusieurs services commerciaux critiques au sein de quelques secteurs d'activité. Les enseignements tirés de ces évaluations pilotes ont été intégrés à la feuille de route globale et au plan d'évaluation des services commerciaux critiques restants. »*

*« Bien que nous ayons un programme continuité/résilience opérationnelle existant, nous reconnaissons qu'il doit être mis à jour pour mieux refléter l'évolution des modèles commerciaux - par ex. travail hybride et utilisation croissante de la technologie. »*

*« En amélioration continue, mais cela demande beaucoup de ressource humaine et financière. »*

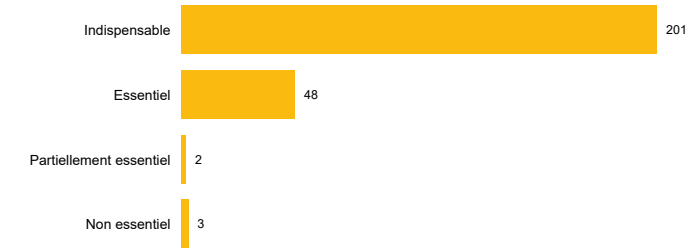
*« (...) il faudra un certain temps à l'organisation pour gagner en maturité et connaître le changement de culture et de mentalité nécessaire pour améliorer notre résilience. »*

*« Nous réorientons notre attention vers les pratiques de continuité des activités et la conception de plans pour commencer à envisager une approche plus holistique de la résilience opérationnelle. »*

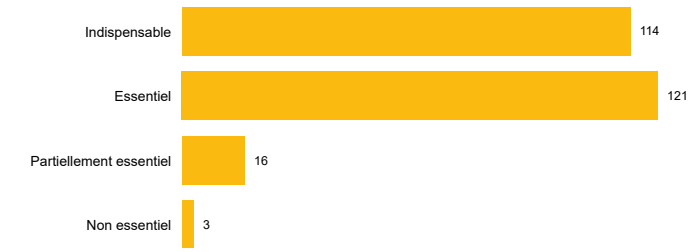
*« L'entreprise connaît une croissance et des changements importants et la résilience est chargée d'alignement et de déploiement pour protéger ces changements et cette expansion. »*

# **Q100-14** Quels processus/activités considérez-vous essentiels à la résilience opérationnelle?

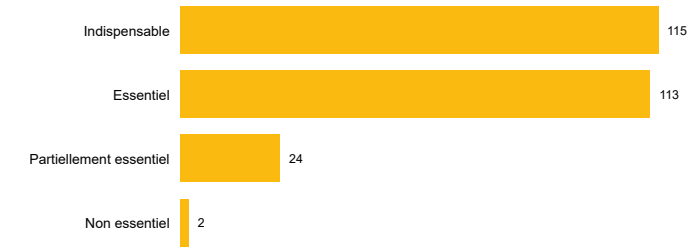
Identifier les services commerciaux importants



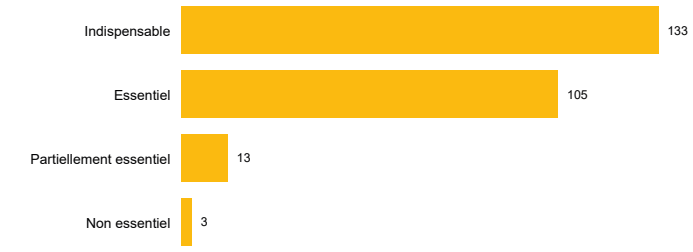

Établir des tolérances d'impact



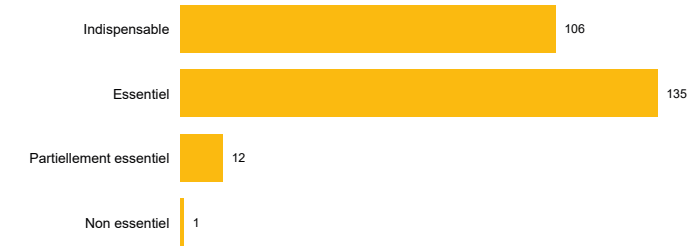

Cartographier les interconnexions et les interdépendances



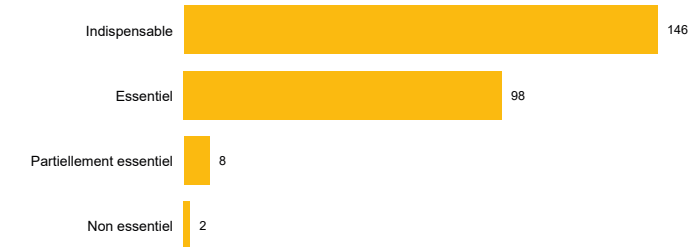

Gouvernance




Gestion des risques opérationnels

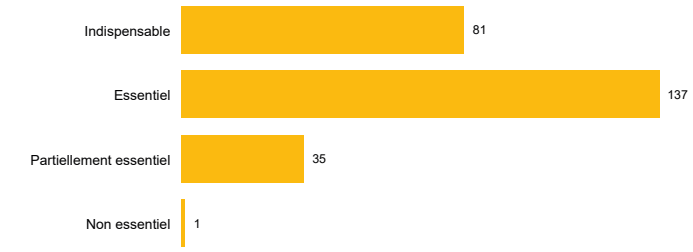



Gestion des dépendances tierces



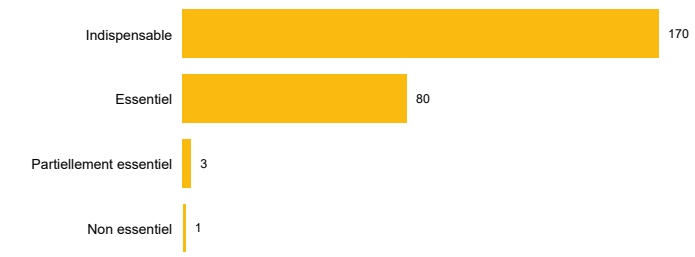

Planification de la continuité des activités

Identifier et utiliser des scénarios plausibles

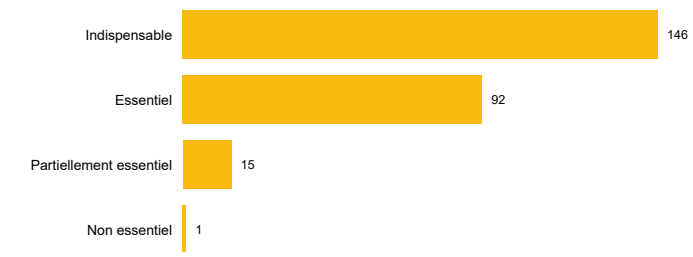


# **Q100-14** Quels processus/activités considérez-vous essentiels à la résilience opérationnelle? (suite)

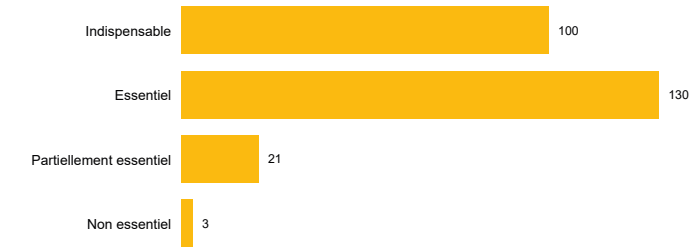
Gestion des TIC / cybersécurité




Gestion des incidents




Hiérarchiser et traiter les vulnérabilités




**Certains des commentaires formulés par les institutions :**

*« Établir une culture qui favorise et renforce les comportements qui soutiennent la résilience opérationnelle, y compris la responsabilité de la haute direction en matière de résilience opérationnelle et la gestion des risques opérationnels associés à leurs opérations critiques. »*

*« Avoir les capacités financières et humaines de faire la planification mais aussi lors de l'évènement. Conserver des réserves financières plus élevées pour y faire face. »*

*« Plans de communications internes et externes, conformité, plan et programme de gestion de crise établis, gestion du changement et gestion des risques liés aux données. »*

## **Q100-15** Quelles difficultés votre institution a-t-elle rencontrées pour établir un programme de résilience opérationnelle?

| Énoncés | Nombre de réponses |
|---|---|
| Nous n'avons pas de programme de résilience opérationnelle | 50 |
| Établissement d'un programme (« par quoi commencer ») | 23 |
| Preuve du retour sur l'investissement | 12 |
| Conception et mise en œuvre initiale du programme | 38 |
| Contraintes liées à la compétence (ressources ayant les connaissances, la formation et l'expérience nécessaire en matière de résilience) | 78 |
| Contraintes liées à l'équipe (ressources dédiées) | 102 |
| Alignement sur un modèle opérationnel cible | 38 |
| Facilitation du programme à l'aide de la technologie | 45 |
| Obtention de changements tangibles/des résultats souhaités | 26 |
| Maintien et avancement du programme (optimisation/investissement continu) | 44 |
| Pas de difficultés à ce jour | 63 |

**Certains des commentaires formulés par les institutions :**

*« Vitesse de changement au sein des attentes des clients et du secteur lui-même, entraînant des changements organisationnels rapides nécessaires pour répondre à ces besoins. »*

*« Malgré la mise en place du cadre de gestion et de gouvernance (…) les attentes en matière de Programme de résilience opérationnelle ne nous semblent pas clairement établies dans les différentes lignes directrices. »*

*« Ces dernières années, les exigences réglementaires et celles des clients ont facilité la justification des dépenses et des efforts (…) Investissements stratégiques dans la technologie à mesure que la pratique de résilience opérationnelle mûrit. »*

*« Lors du recrutement, nous avons constaté que le Canada est un marché immature pour les ressources en résilience opérationnelle qualifiées et expérimentées. »*

*« Priorisation du programme par les parties prenantes ayant d'autres priorités concurrentes. »*

## **Q100-16** Comment évaluez-vous la priorité de la résilience opérationnelle pour votre institution au cours des 12 prochains mois?

**Certains des commentaires formulés par les institutions :**

*« La résilience opérationnelle se développe parallèlement à l'évolution de la stratégie commerciale et de l'appétit pour le risque de l'entreprise. La résilience se situe à l'intersection de nombreux domaines et continuera donc d'être une priorité très élevée pour garantir la durabilité à court, moyen et long terme. »*

*« Compte tenu de l'importance du sujet en raison des risques externes potentiels auxquels notre organisation et l'industrie sont confrontées (…) une approche progressive avec des jalons qui doivent être atteints sur un calendrier particulier. »*

*« En plus de l'embauche récente d'un nouveau responsable du risque opérationnel et de la résilience, il y a toujours des défis à relever pour maintenir et augmenter la RO en tant que priorité élevée. »*

## **Q100-17** Dans quelle mesure l'approche de votre institution en matière de résilience opérationnelle est-elle intégrée?

**Certains des commentaires formulés par les institutions :**

*« Nous avons plusieurs fonctions différentes qui travaillent collectivement ensemble pour contribuer à la résilience opérationnelle, à savoir nos équipes de continuité des activités, de résilience commerciale et technologique, de reprise après sinistre, de sécurité de l'information, de gestion des risques liés aux tiers et de cyberrisques tiers. »*

*« Des équipes dédiées à la mission de la résilience opérationnelle sont en place, accompagnées d'un financement centralisé permettant de livrer nos stratégies de résilience. L'objectif est également intégré à l'ensemble de nos stratégies liées aux technologies de l'information et à la continuité des activités, comme la modernisation de nos systèmes informatiques. Les équipes et instances des trois lignes de défenses sont également impliquées dans le Programme de rehaussement de la résilience. De plus, des réflexions sont en cours pour poursuivre nos efforts d'intégration. »*

*« La Direction externalise la gestion des opérations, y compris la résilience des opérations, à un tiers, et la réponse reflète l'approche de ce tiers. »*

## **Q100-18** Que fait votre institution pour réunir la résilience opérationnelle et d'autres fonctions/disciplines connexes telles que la gestion des dépendances tierces, l'informatique/le cyberrisque, la continuité des activités?

| Énoncés | Nombre de réponses |
|---|---|
| Nous rendons tous compte à la même personne | 65 |
| Rapports doubles/croisés | 89 |
| Collaboration par le biais d'un comité/structure de travail interne | 214 |
| Incertain/pas au courant | 5 |
| Rien | 6 |

**Certains des commentaires formulés par les institutions :**

*« Dans le cadre de la gestion des risques, il existe des groupes spécifiques dédiés à la gestion de diverses fonctions et disciplines telles que la gestion des tiers, l'informatique/le cyberrisque, la continuité des activités, tous relevant du comité de conformité. »*

*« Le programme de continuité des activités et de résilience est examiné et revisité par le biais d'une structure de travail au sein de l'équipe informatique, y compris également les commentaires des directeurs exécutifs, financiers et juridiques. Toute modification ou révision majeure apportée à la Politique est également informée du Comité d'Audit et des Risques et du Conseil. »*

*« Consultants engagés pour aider à évaluer et formuler des recommandations en intégrant les considérations de résilience opérationnelle dans d'autres fonctions (TPRM, technologie, BCM). La résilience opérationnelle, TPRM et BCM rejoignent le même dirigeant, copropriété de la résilience opérationnelle avec la technologie et la cyber-résilience. »*

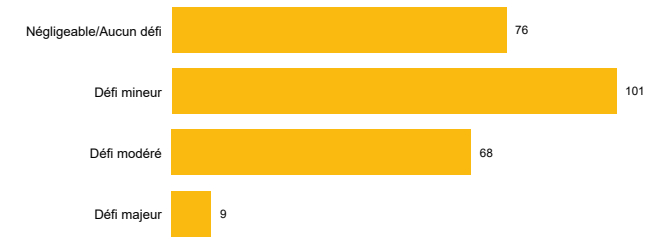
*« La collaboration avec ces fonctions est essentielle au succès du programme Résilience Opérationnelle. Nous organisons des réunions mensuelles de comité de travail et de pilotage auxquelles participent toutes les parties. »*

*« Les unités commerciales et fonctions d'entreprise doivent exiger que tous les fournisseurs tiers critiques maintiennent leurs propres capacités de continuité des activités et maintiennent des niveaux de service suffisants pour répondre à nos exigences critiques. La capacité de réponse du partenaire commercial tiers doit être validée par des exercices avec nous et/ou par la fourniture de preuves suffisantes d'exercices et de tests (...). »*

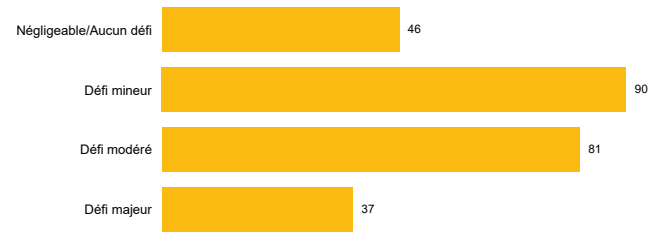
*« L'ensemble de l'équipe de direction rend compte à notre PDG et les questions de résilience opérationnelle sont discutées lors des mêlées bihebdomadaires des dirigeants et des réunions mensuelles du comité des risques ERM. »*

# **Q100-19** Selon vous, quels sont les principaux défis à relever pour mettre en œuvre la résilience opérationnelle au sein de votre institution?

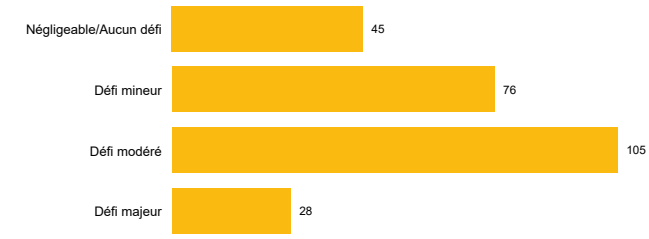
Compréhension incohérente des parties prenantes



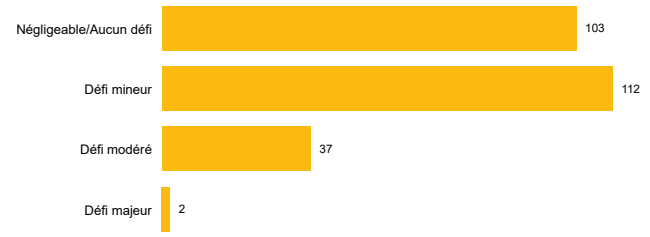

Traiter l'infrastructure héritée



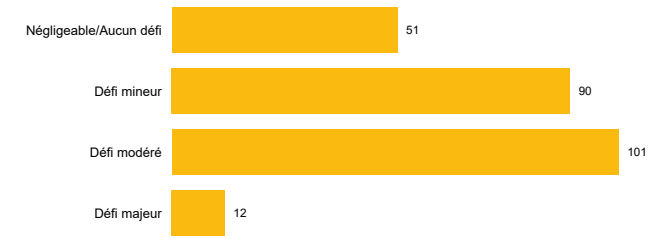

Ne pas avoir les effectifs et/ou le temps du personnel



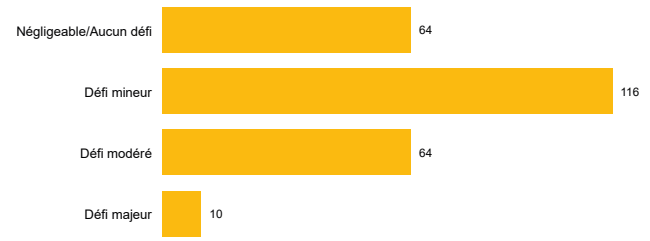

Gouvernance et responsabilisation : avoir les bonnes personnes



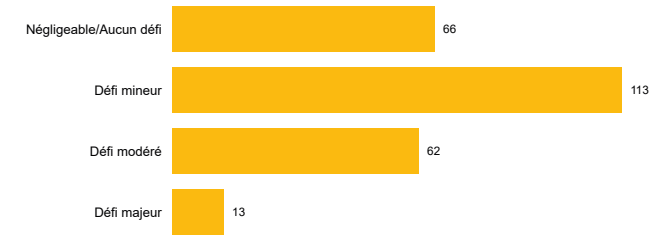

Comprendre, gérer les risques de la chaîne d'approvisionnement



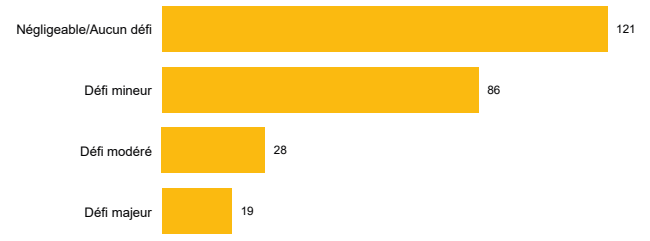

Définition correcte et/ou Réaliste des tolérances d'impact




Cartographier les services commerciaux importants à un niveau suffisant pour identifier les vulnérabilités

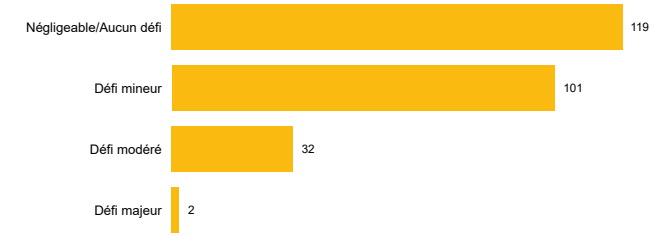



Manque de conseils de la part des régulateurs et/ou gouvernements

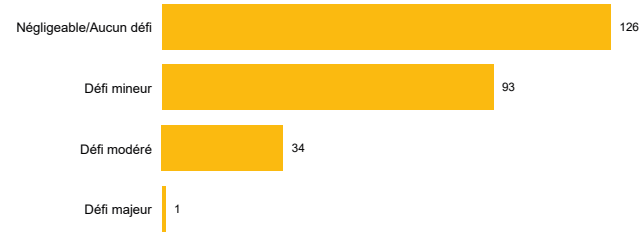


# **Q100-19** Selon vous, quels sont les principaux défis à relever pour mettre en œuvre la résilience opérationnelle au sein de votre institution? (suite)

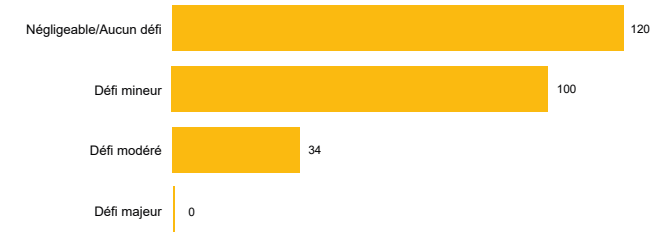
Choisir des scénarios de test sévère mais plausible



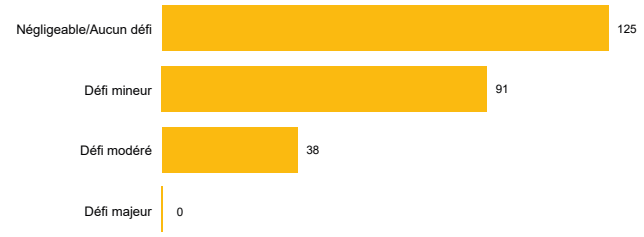

Signaler et apprendre des perturbations et des quasi-accidents



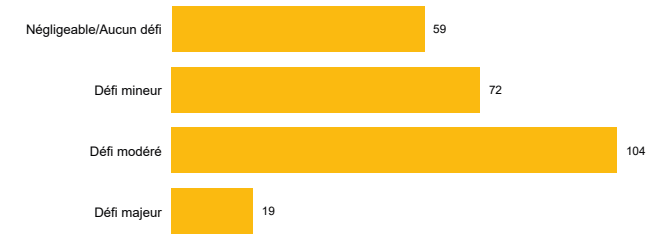

Identifier et convenir des services commerciaux importants




Aucune exigence dans le secteur d'être résilient sur le plan opérationnel




Intégrer la résilience opérationnelle dans la culture de l'organisation




**Certains des commentaires formulés par les institutions :**

*« Un certain manque de sensibilisation et de compréhension de la résilience opérationnelle au sein de l'organisation rend difficile l'établissement de priorités par rapport à d'autres engagements de mise en œuvre. »*

*« Un manque potentiel de cohérence dans l'approche des différents régulateurs pourrait constituer un défi modéré pour une organisation internationale et réduire l'efficacité globale des programmes opérationnels de résilience. »*

*« (…) pour intégrer la résilience opérationnelle au sein de l'organisation, il faut que les documents de gouvernance fondamentaux soient en place, que les outils GRC et de reporting soient en place et que l'organisation soit mature. »*

*« Identifiez le bon équilibre entre la mise en œuvre de la résilience opérationnelle d'un côté et le maintien de la flexibilité et de l'efficacité dans la manière dont les activités sont menées de l'autre côté. »*

*« Une partie du défi résidera dans notre dépendance et dans le nombre de tiers. »*

## **Q100-20** Comment voyez-vous votre institution utiliser les résultats de la résilience opérationnelle (max. 5 priorités)?

| Énoncés | Priorité 1 | Priorité 2 | Priorité 3 | Priorité 4 | Priorité 5 | Total |
|---|---|---|---|---|---|---|
| Prise de décision par le conseil d'administration/l'exécutif | 37 | 15 | 9 | 9 | 20 | 90 |
| Planification des investissements | 10 | 21 | 21 | 19 | 30 | 101 |
| Fournir une assurance conseil/exécutif | 11 | 13 | 15 | 9 | 29 | 77 |
| Aider les plans de reprise/continuité d'activité | 34 | 30 | 23 | 33 | 21 | 141 |
| Satisfaire aux exigences réglementaires | 19 | 12 | 23 | 36 | 36 | 126 |
| Traiter les dommages causés aux clients en cas de perturbation | 60 | 29 | 31 | 26 | 17 | 163 |
| Coordonner activement et régulièrement avec les autres disciplines du risque | 4 | 4 | 12 | 20 | 13 | 53 |
| Identifier les vulnérabilités qui pourraient entraîner une augmentation de la fréquence des perturbations | 37 | 49 | 45 | 43 | 22 | 196 |
| Planification de la perturbation des services commerciaux et mesure de la capacité de récupération | 50 | 64 | 29 | 33 | 12 | 188 |
| Évaluer et atténuer les effets de la perturbation de la chaîne d'approvisionnement | 3 | 11 | 34 | 12 | 40 | 100 |
| Je ne sais pas | 2 | 1 | | | | 3 |

**Certains des commentaires formulés par les institutions :**

*« Bien que nous ayons identifié notre top 5, nous reconnaissons que les résultats opérationnels en matière de résilience soutiendront la majorité des éléments énumérés ci-dessus. »*

*« Nous avons interprété les résultats de résilience opérationnelle comme signifiant les 5 principaux objectifs du programme BC/OpRes. Nous ne considérons pas OpRes comme un programme/domaine distinct, mais comme l'objectif de programmes bien conçus et intégrés pour la continuité des activités, la gestion des risques liés aux tiers, la cybersécurité, etc. »*

*« Tous ces éléments sont une priorité pour notre organisation et sont considérés comme faisant partie de notre feuille de route Op Res. »*

*« Les résultats des évaluations des risques, du suivi financier, opérationnel, culturel et technologique sont des apports directs au cadre de résilience. »*

## **Q200-1** La stratégie de résilience opérationnelle est-elle documentée/formalisée au sein de votre institution?

| Énoncés | Nombre de réponses |
|---|---|
| Une stratégie complète et documentée de résilience opérationnelle existe. La stratégie est revue et mise à jour périodiquement et inclut l'intégration de la résilience opérationnelle dans la culture plus large de l'institution. | 55 |
| Une stratégie de résilience opérationnelle documentée existe, elle est conforme aux exigences de l'institution et est approuvée au niveau de la direction exécutive et du conseil d'administration. | 63 |
| Il existe une stratégie documentée qui considère la résilience opérationnelle à un niveau élevé. La stratégie n'est pas formalisée mais il existe un consensus général par rapport à l'objectif global et au résultat souhaité. | 90 |
| Aucune stratégie de résilience opérationnelle documentée n'est en place. La résilience opérationnelle n'est pas entièrement comprise et la stratégie est actuellement en cours d'élaboration. | 46 |

**Certains des commentaires formulés par les institutions :**

*« Pour être efficaces, nous estimons qu'il faut une compréhension et une approche cohérentes à l'échelle du groupe en matière de résilience opérationnelle. (…), la mise en œuvre de notre stratégie de résilience opérationnelle et des modalités de gouvernance associées ont été gérées au niveau du groupe (plutôt qu'au niveau de l'entité) »*

*« Nous disposons d'un cadre de résilience opérationnelle qui est examiné et approuvé par le comité de gestion des risques du conseil d'administration sur une base prescrite. »*

*« La résilience opérationnelle est composée de plusieurs cadres, politiques, et plus; par opposition à un programme, une stratégie, un document ou une politique autonome. »*

*« Elle n'est pas formalisée dans la mesure où elle est plutôt morcelée à travers différentes pratiques (continuité, relève, sécurité). Des travaux de consolidation sont effectués par l'équipe de la gestion des risques pour obtenir une vue globale. »*

*« La stratégie de résilience opérationnelle est l'équivalent de la GIR pour nous. »*

*« Nous n'avons pas de stratégie de résilience opérationnelle distincte, mais les stratégies commerciales et technologiques en tiennent compte et sont conçues pour générer des résultats résilients pour les clients, les marchés dans lesquels nous exerçons nos activités et nos parties prenantes. »*

*« La résilience opérationnelle est comprise, mais la documentation formalisée est limitée. »*

## **Q200-2** Comment la résilience opérationnelle est-elle planifiée, mise en œuvre et gérée au sein de l'institution?

| Énoncés | Nombre de réponses |
|---|---|
| Il existe un plan de mise en œuvre clairement défini, qui comprend une exécution en temps opportun. Les plans comprennent des dispositions pour la résilience opérationnelle, y compris les investissements et les améliorations nécessaires pour les services commerciaux importants afin de répondre à l'appétit pour le risque (convenu). Les plans sont revus périodiquement pour combler toute lacune identifiée. | 74 |
| Les plans d'exécution de la stratégie de résilience opérationnelle ont été approuvés (c'est-à-dire que les ressources, les fonds et autres nécessités sont ou seront mis à disposition selon les besoins dans les délais envisagés). | 65 |
| Donner la priorité aux services commerciaux pour la résilience opérationnelle qui ont le potentiel de menacer la viabilité, mais ce travail est toujours en cours. Le projet de mise en œuvre de la stratégie de résilience opérationnelle en est à ses débuts et intègre un dialogue avec les différents métiers. | 77 |
| Il n'existe aucun plan documenté pour mettre en œuvre la stratégie de résilience opérationnelle. La résilience opérationnelle est ad hoc et principalement réactive en réponse à une interruption des services aux entreprises. | 38 |

**Certains des commentaires formulés par les institutions :**

*« La gestion de la continuité est pleinement mise en œuvre au sein du Groupe. La résilience opérationnelle est un nouveau concept à venir qui est étudié notamment à travers DORA et d'autres développements réglementaires similaires. »*

*« La résilience opérationnelle est une priorité dans diverses composantes de notre cadre de gestion des risques ; il ne s'agit pas d'un programme distinct doté d'un plan de mise en œuvre distinct. (...) Il s'agit d'un processus continu intégré aux processus globaux de planification commerciale et stratégique. »*

*« Le plan de résilience opérationnelle est conçu pour s'aligner sur les processus métier, services, produits et technologies critiques qui exécutent et exploitent les opérations critiques de l'organisation. Grâce à l'inventaire des services prioritaires, les scénarios de résilience, les mesures et les activités de tests de résistance seront priorisés, exécutés et signalés. »*

*« Nous sommes en train de mettre en œuvre notre programme de résilience opérationnelle. »*

*« La résilience opérationnelle est un travail en cours ("work in progress"). »*

*« Les plans sont construits et gérés entre des départements matriciels. »*

*« Nous avons établi la norme d'entreprise sur la résilience opérationnelle en décembre 2021, qui décrit notre cadre pour gérer les risques opérationnels non financiers ayant un impact sur la résilience opérationnelle, ainsi qu'un programme de mise en œuvre pluriannuel de soutien, qui est supervisé par le comité directeur de la résilience opérationnelle (réunion bimensuelle). »*

## **Q200-3** L'institution a-t-elle aligné sa structure de gouvernance à ses objectifs de résilience stratégiques et opérationnels?

| Énoncés | Nombre de réponses |
|---|---|
| Il existe des comités de gouvernance formels qui examinent les décisions commerciales liées à la résilience opérationnelle et les exceptions sont périodiquement signalées au conseil. La structure de gouvernance fait l'objet d'un examen d'assurance indépendant par l'audit interne et/ou des parties externes. Le conseil d'administration est efficace pour assurer la gouvernance et le leadership du programme de résilience et pour développer les capacités nécessaires. Les risques, la conformité et l'audit interne rendent compte de manière indépendante au conseil d'administration via des comités des risques et d'audit sur la technologie et la résilience opérationnelle. | 49 |
| La structure de gouvernance a été conçue pour soutenir le modèle d'entreprise et l'appétit pour le risque de l'entreprise et est alignée sur ses objectifs stratégiques de résilience opérationnelle. Le conseil d'administration et la haute direction sont pleinement conscients de leurs responsabilités en matière de maintien d'une surveillance efficace. Les risques, la conformité et l'audit interne rendent compte de manière indépendante au conseil d'administration. | 110 |
| Une structure de gouvernance documentée est en place, mais elle nécessite un alignement supplémentaire sur les objectifs stratégiques et opérationnels de résilience de l'institution. Les rôles et les responsabilités de la haute direction en matière de supervision de l'entreprise et de ses activités ont été définis. Une assurance indépendante sur les questions de résilience opérationnelle a été fournie par une partie externe, mais les résultats doivent être intégrés en interne dans les 3 lignes de défense. | 69 |
| Aucune structure organisationnelle documentée actuellement en place. Les rôles et les responsabilités sont déterminés au cas par cas. | 26 |

**Certains des commentaires formulés par les institutions :**

*« Au niveau de l'entreprise, on a fourni des mises à jour régulières au comité des risques du conseil d'administration sur l'état d'avancement des développements du programme de résilience, qui décrivent les activités clés et les échéanciers pour évaluer la résilience de nos services les plus critiques. »*

*« Il existe un comité de continuité des activités et ses activités sont rapportées au conseil d'administration qui inclut des sujets de résilience. »*

*« Aucune assurance indépendante par une partie externe n'a été effectuée. »*

*« Bien qu'aucune structure spécifique ne soit documentée, la gouvernance et la structure organisationnelle supportant les activités de gestion des risques opérationnels sont en grande partie adéquates et suffisantes pour supporter un cadre de résilience opérationnelle. »*

*« La résilience opérationnelle est actuellement en cours de développement. La structure de gouvernance sera alignée sur les objectifs de résilience stratégique et opérationnelle de l'organisation. »*

*« Étant donné que la résilience opérationnelle est actuellement intégrée au programme de gestion des risques opérationnels, la direction a tiré parti de la structure de gouvernance existante au niveau de la direction et du conseil d'administration. »*

*« La gouvernance de la résilience opérationnelle est alignée sur la gouvernance de la gestion des risques opérationnels telle que définie dans la ligne directrice AMF 2016 sur la gestion des risques opérationnels, section 1 - Gouvernance des institutions financières. »*

## **Q200-4** Comment évaluez-vous l'efficacité de votre structure de gouvernance de la résilience opérationnelle?

| Énoncés | Nombre de réponses |
|---|---|
| La structure de gouvernance de la résilience opérationnelle est bien établie et soumise à une assurance indépendante par l'audit interne/des parties externes. Les cadres supérieurs responsables (y compris le conseil d'administration) assurent un leadership efficace du point de vue des défis et de la surveillance. | 56 |
| La structure de gouvernance de la résilience opérationnelle soutient le modèle d'affaires de l'institution et est intégrée dans l'ensemble de l'organisation pour s'aligner sur ses objectifs stratégiques. La haute direction assure une remise en question et une surveillance efficaces si nécessaire. | 105 |
| Structure de gouvernance de la résilience opérationnelle avec rôles et responsabilités définis en place. La structure de gouvernance gagnerait à être mieux alignée sur les objectifs stratégiques de l'institution. | 33 |
| Aucune évaluation formelle entreprise pour évaluer si la structure de résilience opérationnelle est adaptée à son objectif. | 60 |

**Certains des commentaires formulés par les institutions :**

*« L'efficacité de notre programme BC/OpRes est régulièrement évaluée par notre équipe d'audit interne et a récemment été évaluée par un tiers externe. »*

*« Le plan BC est révisé chaque année dans le cadre du SOC 2 ; Des exercices sur table sont menés chaque année avec le soutien d'un soutien externe ; Des évaluations externes de notre Plan BC sont réalisées périodiquement. »*

*« L'évaluation de l'efficacité sera suivie et mesurée à travers l'établissement d'une série d'indicateurs clés de résilience. Ceux-ci seront signalés par l'intermédiaire du comité des risques opérationnels et signalés au comité des risques du conseil d'administration sur une base trimestrielle. On se conforme à la section 2.2 Surveillance et reporting de la ligne directrice 2016 de l'AMF sur la gestion des risques opérationnels. L'efficacité de la structure de gouvernance de la résilience opérationnelle sera également conforme à cette ligne directrice. »*

## **Q200-5** Quel niveau de connaissances et de compétences existe au niveau de la haute direction pour la résilience opérationnelle?

| Énoncés | Nombre de réponses |
|---|---|
| Tous les cadres supérieurs (y compris les membres du conseil d'administration) ont une compréhension suffisante pour assurer une supervision efficace de la stratégie de résilience opérationnelle de l'institution. Au moins un cadre supérieur possède des connaissances et des compétences spécialisées sur lesquelles les autres cadres peuvent s'appuyer. | 122 |
| Au moins un cadre supérieur (y compris les membres du conseil) a une compréhension suffisante pour assurer la supervision de la stratégie de résilience opérationnelle de l'institution. Une formation est prévue pour développer les capacités d'autres cadres supérieurs au cours des 12 prochains mois. | 91 |
| Les cadres supérieurs ont des compétences limitées dans les domaines de la résilience opérationnelle. Il existe une dépendance à l'égard des connaissances et des compétences externes pour combler les lacunes et assurer une surveillance efficace de la stratégie de résilience opérationnelle de l'institution. Il existe un plan pour améliorer les compétences / nommer des cadres supérieurs ayant une expérience pertinente au cours des 12 prochains mois. | 14 |
| Aucun cadre supérieur n'a actuellement les connaissances et les compétences nécessaires pour remettre en question et superviser efficacement la stratégie de résilience opérationnelle de l'institution. Il n'y a aucun plan en place pour résoudre ce problème. | 27 |

**Certains des commentaires formulés par les institutions :**

*« Tous les cadres supérieurs et membres du conseil d'administration ont une bonne compréhension de la résilience opérationnelle. (…) dirigeants à tous les niveaux comprennent les rôles et les responsabilités et possèdent les connaissances dont ils ont besoin pour développer et maintenir des plans de reprise opérationnelle efficaces basés sur les priorités de l'entreprise. »*

*« Nous ne sommes pas en mesure de vous répondre précisément sur cette question puisque cela n'a jamais été évalué directement. »*

*« Maintenant que le concept de résilience organisationnel est porté à notre attention, un plan de formation de compétence sera mis en place. »*

*« Les cadres supérieurs et le conseil d'administration ont des connaissances en matière de gestion des risques opérationnels, de continuité des activités et de reprise après sinistre et ont besoin d'être améliorés pour les aspects de la résilience opérationnelle avec une communication/formation appropriée si nécessaire. »*

*« Les connaissances en matière de résilience opérationnelle se situent à différents niveaux au sein de la direction générale et du conseil d'administration. Cependant, le CRO continue de défendre les principes de résilience opérationnelle (…) la formation formelle continue d'être en cours de développement. »*

## **Q200-6** Comment vous assurez-vous que le conseil d'administration et la haute direction assurent une surveillance et une remise en question efficaces?

| Énoncés | Nombre de réponses |
|---|---|
| Le conseil, les comités et la haute direction disposent de toutes les mesures appropriées, ce qui leur permet d'assurer une surveillance et une remise en question efficaces. Les 2e et 3e lignes de défense s'acquittent efficacement de leurs responsabilités de remise en question et de surveillance. L'information de gestion produite permet la prise de décision liée à la gouvernance. | 77 |
| La surveillance exercée par le conseil, les comités et la haute direction est structurée, documentée et normalisée. Les informations de gestion sont utilisées pour informer la haute direction et comme contribution à la plupart des prises de décision. La 3e ligne de défense examine les informations de gestion et fournit une assurance indépendante. | 92 |
| La surveillance exercée par le conseil, les comités et la haute direction est de haut niveau et ponctuelle. Les informations de gestion sont utilisées pour informer la haute direction et comme contribution à certaines prises de décision. | 84 |
| Rien n'indique que le conseil, les comités et la haute direction assurent une surveillance. Des évaluations indépendantes ont mis en évidence un environnement de prise de décision/de prise de décision médiocre. | 1 |

**Certains des commentaires formulés par les institutions :**

*« Le conseil d'administration, les comités et la haute direction de la compagnie supervisent la stratégie de résilience opérationnelle pour les services commerciaux importants. Nous traversons notre premier cycle de vie et établissons actuellement une structure formelle pour OpRes. »*

*« Depuis que nous avons récemment commencé à rendre compte au Conseil, nous nous attendons à ce que les orientations se renforcent au cours des prochains trimestres. Nous prévoyons de présenter des rapports et des mises à jour de routine au Conseil d'administration sur une base trimestrielle pour permettre une remise en question et une surveillance efficaces. »*

*« La surveillance est renforcée dans le cadre des améliorations identifiées au programme. Les 2LOD et 3LOD s'acquittent efficacement de leurs responsabilités de défi et de surveillance. »*

*« Le cadre de la OpRes en est aux premiers stades de mise en œuvre et la surveillance à ce stade a été de haut niveau. Des rapports sur les progrès de la mise en œuvre sont en place, mais les mesures ne sont pas encore communiquées. »*

## **Q200-7** Toutes les responsabilités ont-elles été attribuées au niveau approprié et approuvées par les parties prenantes concernées?

| Énoncés | Nombre de réponses |
|---|---|
| Les rôles et les responsabilités sont intégrés dans les spécifications de poste et la gestion des performances. Les rôles et les responsabilités ont été approuvés et communiqués aux principales parties prenantes, y compris les régulateurs. Les questions telles que les conflits, les doubles emplois et les responsabilités partagées ont été clairement identifiées, documentées et les risques atténués. | 37 |
| Structure en place avec une expertise opérationnelle disponible au niveau du conseil d'administration/de la haute direction. Les rôles et responsabilités clés en matière de résilience opérationnelle sont documentés avec une propriété clairement définie et comprise. | 117 |
| Les personnes responsables de la résilience opérationnelle ont été identifiées en s'appuyant sur des conseillers externes pour compléter et combler les lacunes en matière de connaissances et/ou de compétences (le cas échéant). | 66 |
| Propriété, rôles et responsabilités non entièrement déterminés et compris. Les rôles et les responsabilités sont attribués sur une base réactive. | 34 |

**Certains des commentaires formulés par les institutions :**

*« La gouvernance est existante pour les différentes composantes d'un programme de résilience opérationnelle (ex. : risques des tiers, risques TDSI, etc.). »*

*« Nous faisons également affaires avec des firmes externes (breach coach, forensic et communications). »*

*« Les rôles et responsabilités sont en cours d'examen et de mise à jour dans le cadre des améliorations identifiées au programme. »*

*« Des cadres et pratiques de gouvernance et de risque sont en place au niveau de l'entreprise et au sein des opérations informatiques et de sinistres depuis de nombreuses années, mais ils ne sont pas qualifiés de "résilience opérationnelle". »*

## **Q200-8** Votre personnel et vos cadres supérieurs comprennent-ils les objectifs stratégiques de l'institution et comment les capacités de résilience opérationnelle les facilitent-ils?

| Énoncés | Nombre de réponses |
|---|---|
| Tous les employés sont conscients de l'objectif stratégique d'avoir une institution résiliente sur le plan opérationnel. La discussion sur la résilience opérationnelle est une preuve au niveau du conseil d'administration et est prise en compte dans toutes les activités courantes. La culture de l'entreprise est conçue pour favoriser la résilience opérationnelle, et cela se manifeste dans le comportement du personnel à tous les niveaux. L'éducation et la sensibilisation à la résilience opérationnelle sont prises en compte dans les décisions commerciales. | 42 |
| La plupart des employés sont conscients de l'objectif stratégique d'avoir une institution résiliente sur le plan opérationnel. Des sessions de formation et des séminaires, etc. sont organisés pour améliorer les connaissances du personnel sur la résilience opérationnelle, y compris la formation et la sensibilisation à la sécurité. Il existe certaines preuves que la résilience opérationnelle est ancrée dans la culture de certaines parties de l'entreprise. | 88 |
| Certains membres du personnel (y compris les cadres supérieurs) connaissent les objectifs stratégiques et ont conscience de la résilience opérationnelle. Une formation de base de haut niveau est dispensée, y compris une formation et une sensibilisation à la sécurité. | 103 |
| La stratégie de résilience opérationnelle n'a pas été transmise au personnel. Le personnel ne semble pas conscient de la résilience opérationnelle et aucune formation formelle n'est en place pour combler cette lacune. | 21 |

**Certains des commentaires formulés par les institutions :**

*« Plusieurs programmes qui soutiennent la résilience opérationnelle ont déployé des éléments de formation, y compris des formations obligatoires à tous les employés au sein de l'organisation. »*

*« La société est consciente de l'importance de développer de façon plus poussée la culture relative à la résilience opérationnelle. Le défi majeur est intimement lié au mouvement de personnel que connaissent tous les employeurs. »*

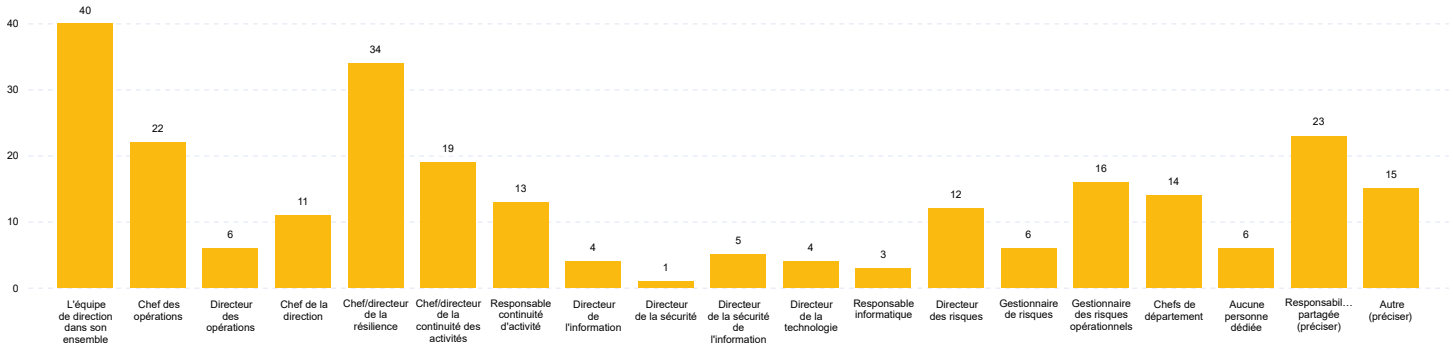
*« Nous avons des exigences de formation à l'échelle de l'entreprise en matière de continuité des activités et de sensibilisation, ainsi qu'un programme annuel de formation en gestion de la conformité. »*

*« La plupart des dirigeants sont conscients de l'importance de la résilience opérationnelle. Davantage de formation, y compris des exercices sur table, sont nécessaires pour garantir la clarté des rôles et des responsabilités. »*

*« La structure est en place, mais elle nécessite un élargissement des possibilités de résilience opérationnelle. »*

*« La préparation aux situations d'urgence a été transmise à tout le personnel ayant reçu une formation - en tant qu'élément de la résilience opérationnelle. »*

## **Q200-9** Personne prenant la tête au jour le jour de la résilience opérationnelle au sein de l'institution?




**Certains des commentaires formulés par les institutions :**

*« Cet élément n'est pas officialisé encore. La responsabilité sera potentiellement aux propriétaires des opérations vitales identifiées. Le Chef de la gestion des risques aura également une responsabilité de propriétaire de cadre. »*

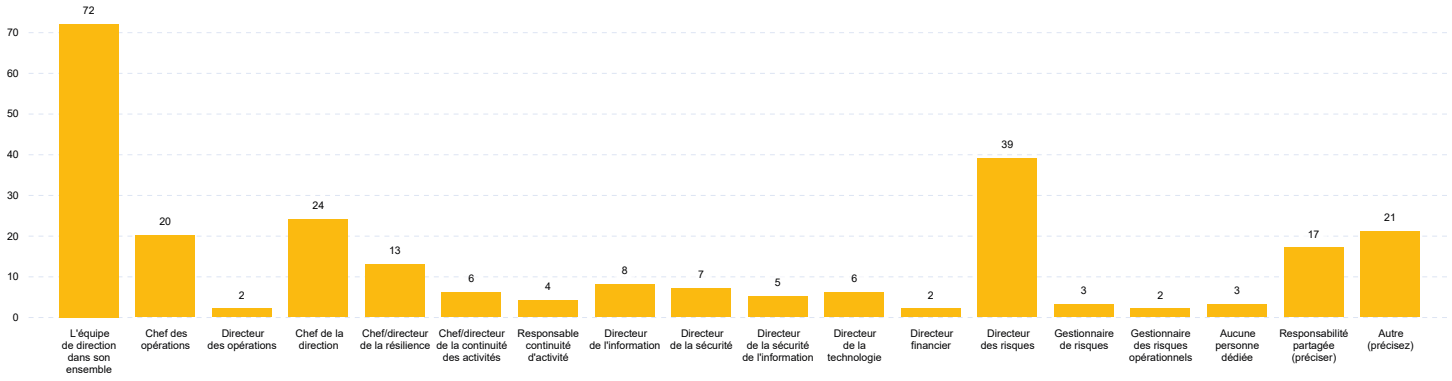
*« La résilience opérationnelle n'est pas la responsabilité d'une seule personne. Il existe une responsabilité partagée au niveau du groupe entre : le responsable mondial de la résilience de l'entreprise, le responsable de la sécurité de l'information (CISO), le responsable de la gestion des risques liés aux tiers (TPRM), le responsable du risque opérationnel, le responsable informatique et les responsables de toutes les activités concernées. Cette responsabilité est en grande partie assumée au niveau de l'entité par le chef des services commerciaux. »*

*« Le responsable de la continuité des activités est responsable de la maintenance des outils et processus BC. Le personnel de gestion des risques veille à ce que les autres cadres de gestion des risques (par exemple, cybersécurité, tiers) reflètent de manière appropriée les priorités opérationnelles en matière de résilience. »*

*« La Direction confie la gestion de ses opérations, y compris la résilience opérationnelle, à un tiers. »*

*« Nous avons également récemment embauché un nouveau responsable du risque opérationnel et de la résilience, qui sera également impliqué dans cette activité. »*

## **Q200-10** Personne ayant la responsabilité globale de la résilience opérationnelle au sein de l'institution?




**Certains des commentaires formulés par les institutions :**

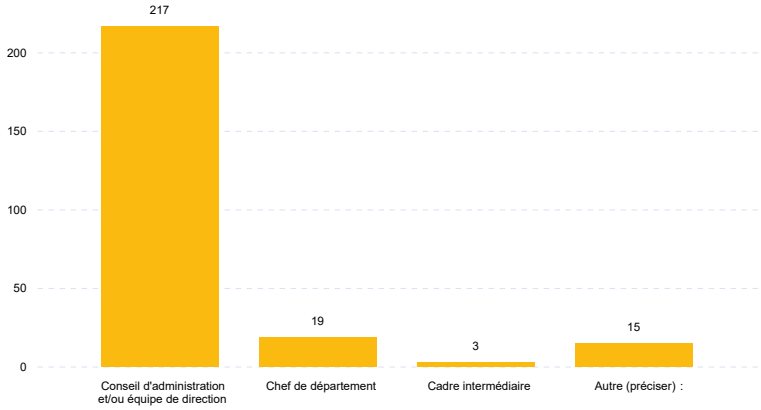
*« Le risque sera détenu par la première ligne – probablement par un membre de l'exécutif, sinon le PDG. »*

*« La composante la plus développée de la résilience opérationnelle se situe actuellement au sein du département informatique. A ce titre, le responsable informatique est le plus proche de cette fonction. (…) structure davantage clarifiée à mesure que nous développerons notre programme de résilience opérationnelle. »*

*« Le CIO est responsable des cadres de BC et de cybersécurité, ainsi que d'une partie de la gestion des risques liés aux tiers. Le CRO est chargé de veiller à ce que la résilience opérationnelle soit reflétée dans tous les cadres applicables. »*

*« Responsabilité partagée entre le Business Resilience Office, la gestion des risques, la sécurité de l'information, la gestion des incidents et la reprise après sinistre. »*

## **Q200-11** Quel est le niveau de la personne ayant la responsabilité globale de la résilience opérationnelle au sein de votre institution?



## **Q200-12** Que pensez-vous de la création d'une nomination au niveau du conseil d'administration chargée d'évaluer la résilience à tous les niveaux et de veiller à ce que tous les efforts de renforcement de la résilience au sein de l'institution soient alignés et coordonnés?

**Certains des commentaires formulés par les institutions :**

*« Un sous-comité du conseil d'administration a la charge de l'ensemble des risques de l'organisation. »*

*« La résilience opérationnelle est une responsabilité de la haute direction (…) Il n'y a aucun avantage à centraliser ce sujet auprès d'une seule personne lors du conseil d'administration. »*

*« Doit relever du comité de gestion des risques. Le président de ce comité est déjà au CA. »*

*« Nous examinerons la structure appropriée à mesure que nous continuerons à mettre en œuvre notre programme de résilience opérationnelle. »*

*« Nous croyons, respectueusement, que le conseil d'administration doit effectivement être informé des démarches entreprises, mais qu'une telle fonction (évaluation de la résilience opérationnelle) devrait plutôt relever de la direction. »*

*« Nous ne pensons pas que cela soit nécessaire. Le rôle du conseil d'administration est de superviser les principaux risques de l'organisation, y compris la résilience opérationnelle.*

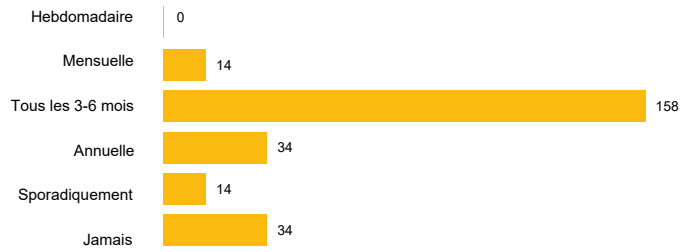
*« Le conseil d'administration devrait fournir une remise en question constructive et une surveillance de ces activités comme il le fait pour d'autres activités commerciales. »*

*« Le conseil d'administration remet en question les aspects de résilience opérationnelle sans poste dédié. »*

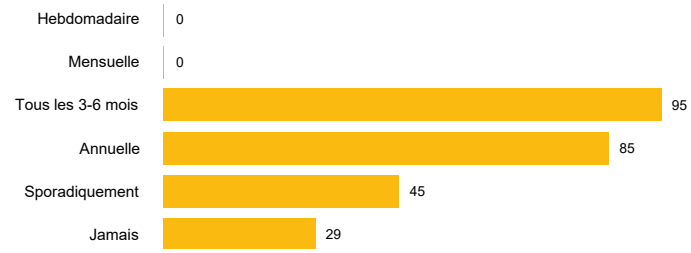
*« Un membre du conseil d'administration s'est vu confier la responsabilité du programme de résilience opérationnelle, avec des dispositions de gouvernance en place pour assurer la surveillance des cadres de risque plus larges/connexes. »*

# **Q200-13** À quelle fréquence la résilience opérationnelle figure-t-elle à l'ordre du jour des comités suivants ou de leur équivalent le plus proche dans votre institution?

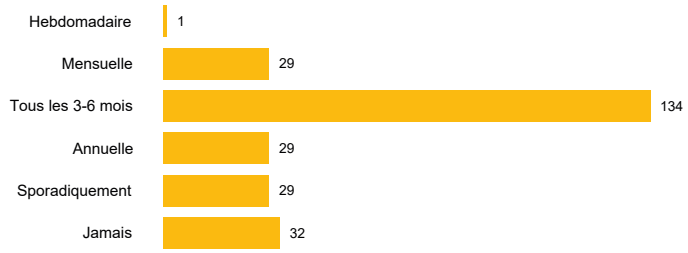
Comité des risques



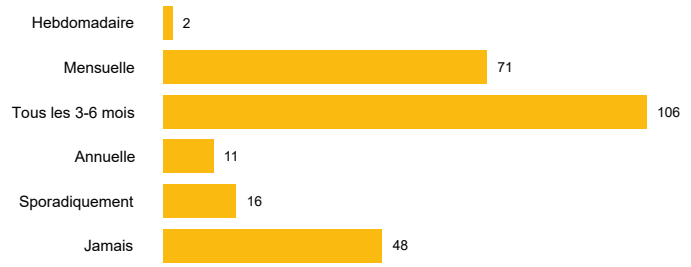

Conseil




Comité exécutif




Comité des risques technologiques




**Certains des commentaires formulés par les institutions :**

*« Nous commencerons à rendre compte du programme de résilience opérationnelle au conseil d'administration (…) Actuellement, le reporting du programme est effectué sur une base ad hoc au comité d'exploitation et des mises à jour mensuelles sont fournies au comité des risques opérationnels. »*

*« Notre CRO rend compte trimestriellement à notre comité de conformité, de risque et de révision de la conduite des risques, ce qui inclut la continuité des activités et d'autres risques liés à la résilience opérationnelle. »*

*« Actuellement, la résilience opérationnelle est régulièrement à l'ordre du jour du conseil d'administration. »*

*« En raison de l'importance de cette initiative, elle est présentée à tous les membres du Conseil d'administration. Nous n'avons pas de comité des risques technologiques. »*

*« La direction confie la gestion de ses opérations, y compris la résilience opérationnelle, à un tiers. Le tiers ne dispose pas de comité des risques dédié ni de comité des risques technologiques. (…) Le comité exécutif tiers discute de la continuité des activités, si nécessaire, au moins une fois par an. »*

*« Localement, nous n'avons pas de comité des risques dédié ni de comité des risques technologiques. Notre conseil d'administration discute de la continuité des activités au moins une fois par an, mais la transition vers la résilience opérationnelle n'a pas encore eu lieu. (…) À l'échelle mondiale : notre comité des risques opérationnels examine divers éléments de notre programme OpRes en moyenne 2 à 3 fois par an. »*

*« Il n'y a pas de rythme défini pour que la résilience opérationnelle soit inscrite à l'ordre du jour – les sujets liés à la résilience opérationnelle sont abordés, selon les besoins. En moyenne, l'option 3 (tous les 3 à 6 mois) serait la réponse la plus appropriée. Cependant, il y a des moments où la résilience opérationnelle peut être plus fréquemment à l'ordre du jour. En outre, nous disposons d'un Conseil de résilience d'entreprise qui se réunit toutes les trois semaines. »*

## **Q200-14** Comment caractériseriez-vous votre budget annuel affecté à votre contingence de résilience opérationnelle?

**Certains des commentaires formulés par les institutions :**

*« Étant donné que nous n'avons pas de programme, aucun budget n'est alloué. Le tout fait partie de nos dépenses opérationnelles. »*

*« Nous disposons d'un budget d'urgence en matière de cybersécurité. D'autres éventualités liées à la résilience opérationnelle seraient financées à partir du capital disponible. »*

*« Le financement a été accordé en priorité à la résilience opérationnelle. Nous avons approuvé un financement pour les 15 prochains mois et demanderons un financement supplémentaire par la suite. »*

*« Nous disposons de budgets opérationnels spécifiques pour les équipes responsables de divers aspects de notre programme global de résilience opérationnelle. »*

*« Il n'existe actuellement aucun budget dédié spécifiquement à la résilience opérationnelle, mais lorsqu'il existe des initiatives distinctes à l'appui des éléments de résilience opérationnelle, la réserve pour imprévus suivrait les pratiques de gestion de projet. »*

*« Un budget est en place pour la gestion de la continuité des activités, y compris la technologie et une ressource dédiée, mais doit être élargi pour la résilience opérationnelle. »*

*« Le Conseil reconnaît que des ressources financières supplémentaires sont nécessaires pour répondre à ce besoin croissant. »*

## **Q200-15** Comment caractérisez-vous l'évolution de votre budget annuel pour la résilience opérationnelle au cours des 12 prochains mois?

**Certains des commentaires formulés par les institutions :**

*« Nous n'avons pas l'intention d'ajuster substantiellement nos budgets opérationnels actuels. L'excédent de notre entreprise est actuellement suffisant pour résister à un large éventail d'événements de perturbation opérationnelle. »*

*« Il n'existe actuellement aucun budget dédié spécifiquement à la résilience opérationnelle, mais il existe des initiatives distinctes pour soutenir le renforcement des éléments de résilience opérationnelle contenus dans les budgets du risque opérationnel, de la technologie et de l'entreprise. »*

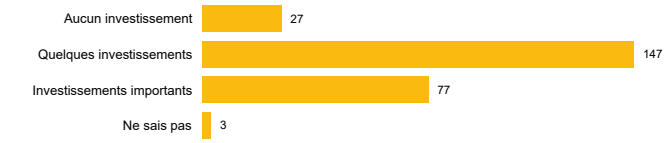
*« Nous prévoyons que nos besoins financiers augmenteront à mesure que nous développerons le programme. »*

*« À mesure que les orientations réglementaires deviennent plus claires avec une date d'entrée en vigueur définie, nous envisagerions également d'allouer davantage de ressources à la résilience opérationnelle. »*

*« À mesure que nous continuons à croître et à investir dans l'organisation, les plans et les objectifs de résilience seront pris en compte dans ce processus afin d'éviter de "rattraper notre retard". »*

# **Q200-16** Niveau des investissements réalisés au cours des DEUX DERNIÈRES ANNÉES par votre institution dans les domaines suivants?

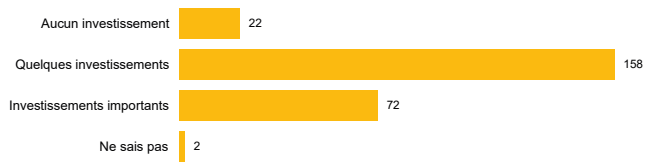
Cartographie des processus critiques



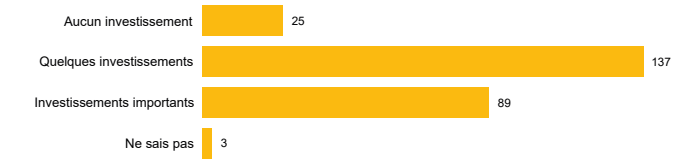

Identification et gestion des menaces et vulnérabilités des opérations critiques

Planification et test de la continuité des activités

Identification des interconnexions et interdépendances

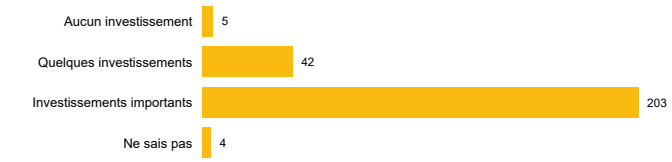



Gestion des dépendances tierces pour la livraison des opérations critiques




Gestion des incidents

Programmes de protection, de détection, d'intervention et de récupération pour la résilience des TIC et de la cybersécurité



# **Q200-17** Niveau des investissements prévus au cours des DEUX PROCHAINES ANNÉES par votre institution dans les domaines suivants?

Cartographie des processus critiques

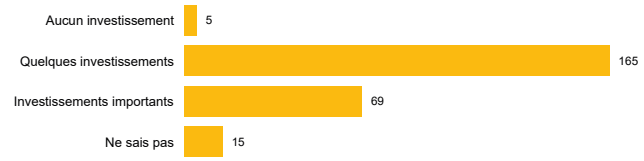
Identification et gestion des menaces et vulnérabilités des opérations critiques

Planification et test de la continuité des activités

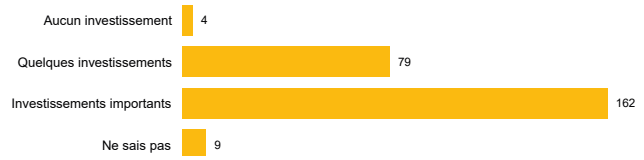
Identification des interconnexions et interdépendances

Gestion des dépendances tierces pour la livraison des opérations critiques

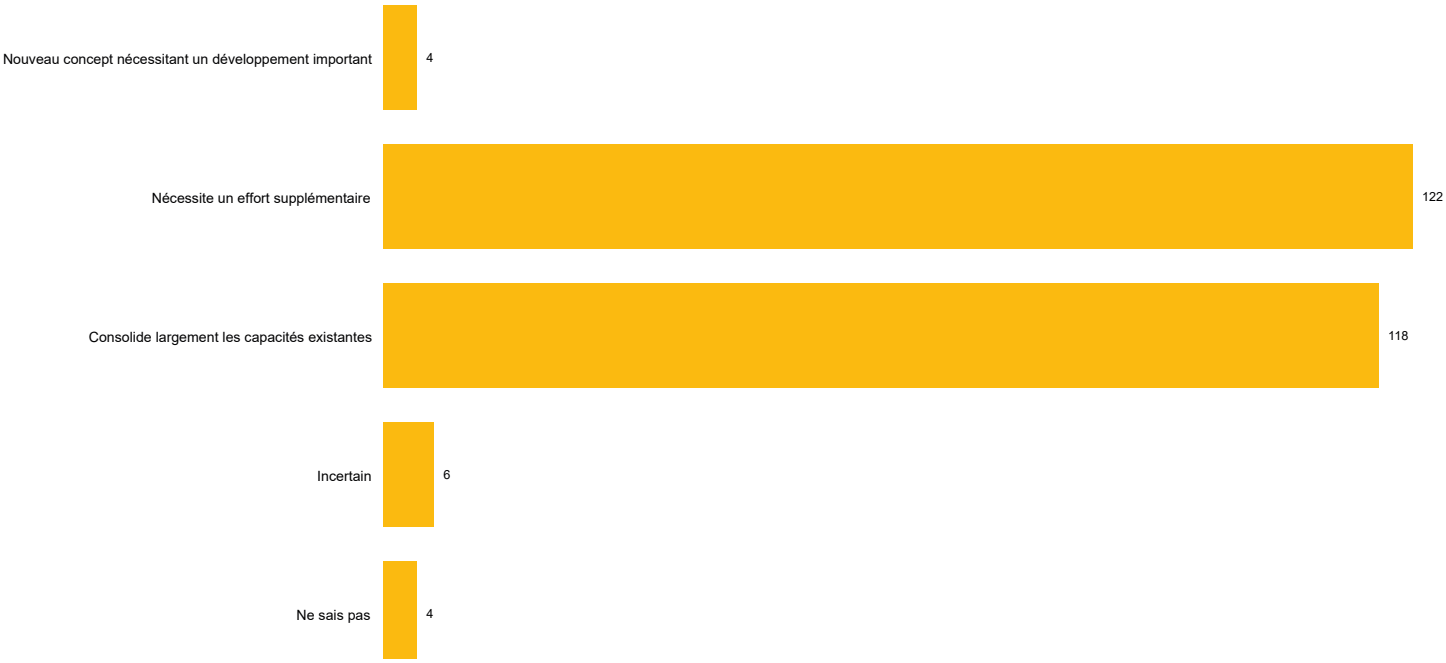
Gestion des incidents




Programmes de protection, de détection, d'intervention et de récupération pour la résilience des TIC et de la cybersécurité



## **Q200-18** Quel impact la résilience opérationnelle a-t-elle sur vos capacités de gestion des risques existante?




**Certains des commentaires formulés par les institutions :**

*« Notre cadre de gestion des risques est assez mature, mais nous devons y intégrer plus explicitement la réflexion sur la résilience opérationnelle. »*

*« La résilience fait partie intégrante de nos pratiques de gestion de risques opérationnels. Toutefois, des renforcements sont en cours dans la systématisation de l'approche, notamment au niveau des projets. »*

*« C'est un concept nouveau pour nous, il faudra y consacrer des efforts supplémentaires. »*

*« Nous sommes en train de réviser nos processus et procédures en place afin de nous assurer d'identifier correctement les risques critiques et d'ajuster notre manière d'y faire face. »*

*« La prise en compte de la résilience opérationnelle doit être intégrée aux capacités existantes de gestion des risques. »*

*« Nous n'avons pas encore pu mesurer l'ampleur des efforts supplémentaires qui seront nécessaires car nous n'avons pas terminé le plan. »*

*« Nos capacités de gestion des risques sont suffisantes pour soutenir l'intégration continue de la résilience opérationnelle dans l'organisation. Cependant, (…) la modification de nos pratiques doit passer par plusieurs mécanismes de gouvernance établis au sein de l'institution. »*

## **Q200-19** Disposez-vous d'une structure organisationnelle et d'un processus de gouvernance établis pour gérer le risque de résilience opérationnelle et décrit-il les responsabilités et les obligations?

| Énoncés | Nombre de réponses |
|---|---|
| La fonction de gestion des risques de résilience opérationnelle a été établie et pleinement intégrée dans l'ensemble de l'organisation avec une articulation claire des rôles et des responsabilités. La structure et le processus de gouvernance ont été examinés de manière indépendante avec des preuves documentées. Le conseil est conscient des principaux risques, y compris ceux qui dépassent l'appétit pour le risque et/ou qui nécessitent une approbation. | 39 |
| L'organigramme décrivant la structure de gestion des risques de résilience opérationnelle est en place. Une structure et un cadre de gouvernance ont été établis décrivant l'approche globale et sont alignés sur les objectifs stratégiques. Comités pertinents et structures hiérarchiques en place avec nomination d'un haut responsable. Cette personne est le dirigeant responsable et supervise le risque de résilience opérationnelle. Les informations de gestion sont produites et partagées périodiquement avec la haute direction. | 103 |
| La structure et le cadre de gouvernance de la résilience opérationnelle ont été établis mais pas entièrement intégrés. Les rôles et les responsabilités ont été définis et attribués aux personnes clés. Un dirigeant responsable sera nommé en temps voulu. Les informations de gestion sont produites sur une base ad hoc et partagées avec la haute direction. | 59 |
| La structure de gouvernance de la résilience opérationnelle n'existe pas. Nous sommes en train d'établir le processus de gouvernance pour gérer le risque de résilience opérationnelle. | 53 |

**Certains des commentaires formulés par les institutions :**

*« La résilience s'inscrit dans notre gouvernance et gestion de risques technologiques, dont les rôles et responsabilités ont été renforcés au cours des dernières années. Les encadrements sur l'appétit du risque s'appliquent également sur les risques de résilience. »*

*« Il n'existe pas d'organigramme décrivant la structure de gestion des risques de résilience opérationnelle. »*

*« Une enquête actuelle est en cours, dans le but de tirer parti de la structure de gouvernance existante de la gestion de la continuité des activités d'entreprise. »*

*« Nous chercherons à évaluer et à exploiter notre cadre de gouvernance existant en matière de résilience d'entreprise. »*

*« Une fois mis en œuvre, nous formaliserons une structure de gouvernance pour permettre un reporting efficace et créer de la visibilité. »*

*« Un modèle de gouvernance avec des rôles et des responsabilités est en cours d'examen (...) La gouvernance de la résilience opérationnelle est alignée sur la gouvernance de la gestion des risques opérationnels telle que définie dans la Ligne directrice 2016 de l'AMF sur la gestion des risques opérationnels, section 1 – Gouvernance des institutions financières. »*

## **Q200-20** Dans quelle mesure les informations de gestion, y compris les indicateurs de risque clés, sont-elles utilisées pour informer les décideurs sur la performance des contrôles de résilience opérationnelle?

| Énoncés | Nombre de réponses |
|---|---|
| Les cadres supérieurs examinent périodiquement les informations de gestion sur les contrôles de résilience opérationnelle. Les informations de gestion sont également utilisées pour informer la haute direction sur les questions clés liées à la résilience opérationnelle et pour la prise de décision pertinente. Les indicateurs clés de risque sont revus après chaque événement significatif. Ces informations de gestion, associées à l'auto-évaluation des risques et des contrôles, sont utilisées pour évaluer l'efficacité de l'environnement de contrôle et pour la prise de décision pertinente. | 67 |
| Le personnel de la 2e ligne de défense, tel que les responsables des risques opérationnels, examine périodiquement les informations de gestion sur les contrôles de résilience opérationnelle en conjonction avec l'auto-évaluation des risques et des contrôles afin d'évaluer l'efficacité des processus de contrôle interne. | 80 |
| Cadre de contrôle des risques développé et mis en œuvre dans toute l'organisation. Le personnel de 1re ligne, tel que les responsables technologiques ou opérationnels, examine périodiquement les informations de gestion sur les contrôles de résilience opérationnelle pour prendre des décisions éclairées. | 49 |
| Les informations de gestion pour les contrôles de résilience opérationnelle sont saisies de manière ad hoc et ne sont pas périodiquement révisées. | 58 |

**Certains des commentaires formulés par les institutions :**

*« Le développement de contrôles spécifiques à la résilience opérationnelle au-delà des contrôles existants en matière de technologie, de cybersécurité et de risque de tiers est en cours de développement. »*

*« Des KRI sont en place et rapportés trimestriellement. »*

*« Les considérations relatives aux informations de gestion formalisées pour les contrôles seront intégrées dans la construction future du programme. »*

*« Il s'agit d'un travail en cours qui nécessite d'être amélioré pour la résilience opérationnelle. »*

*« Des indicateurs de risque clés sur la résilience opérationnelle sont intégrés dans les comités de haute direction, tels que le comité de gestion informatique et le comité des risques et de la conformité. »*

## **Q300-1** Votre institution financière a-t-elle identifié et documenté des services commerciaux importants qui, s'ils étaient interrompus, pourraient nuire aux consommateurs ou à l'intégrité du marché?

**Certains des commentaires formulés par les institutions :**

*« Les activités critiques de l'ensemble des secteurs de l'organisation sont identifiées et leur tolérance d'interruption établie selon, entre autres, l'impact sur la relation d'affaires et la satisfaction des clients. »*

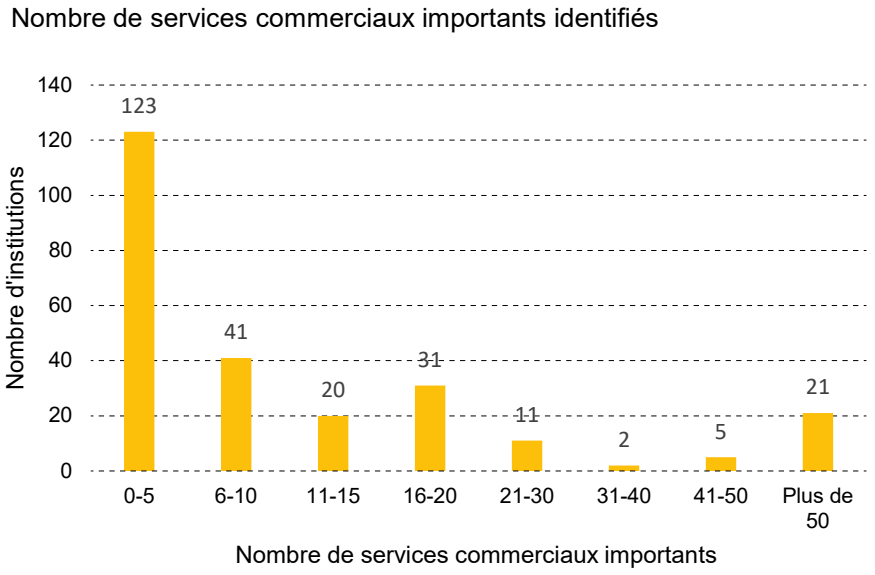
*« Nous avons identifié 20 services essentiels au sein de l'entreprise mondiale qui, s'ils étaient interrompus, causeraient des niveaux de préjudice intolérables aux clients, à l'intégrité des marchés, à la stabilité financière et/ou menaceraient la sécurité et la solidité de l'institution. »*

*« Même si les processus critiques sont identifiés, ils concernent les opérations de l'entreprise et non les dommages causés aux consommateurs ou à l'intégrité du marché. »*

*« Il est difficile de répondre à cette question, car les "services commerciaux importants" peuvent avoir une signification différente selon les organisations. »*

*« Tous les services commerciaux ont été identifiés et classés en fonction de l'impact sur le client, de l'impact sur les employés et d'autres considérations. »*

## **Q300-2** Combien de services commerciaux importants votre institution a-t-elle identifiés?



## **Q300-3** Comment vous assurez-vous que les services commerciaux importants identifiés sont au niveau auquel une tolérance d'impact peut être appliquée et permettent aux conseils d'administration et à la haute direction de prendre des décisions de priorisation et d'investissement?

| Énoncés | Nombre de réponses |
|---|---|
| Il y a une bonne compréhension des services commerciaux et de leur impact potentiel. Les services ont été identifiés au niveau individuel - ils ne sont pas subdivisés en plusieurs services. L'impact est clairement compris et la tolérance a été fixée au bon niveau. Des informations de gestion sont produites régulièrement pour informer les parties prenantes concernées. Les services commerciaux sont identifiés de manière à permettre aux conseils d'administration et à la haute direction de prendre des décisions d'établissement des priorités et d'investissement. | 94 |
| Il existe certaines lacunes dans la compréhension des services commerciaux et de leur impact potentiel en cas de perturbation opérationnelle. Les informations de gestion sont remplies sur une base ad hoc et le conseil d'administration et la haute direction sont au courant du processus de gouvernance pour leur permettre d'établir des priorités et de prendre des décisions éclairées. | 115 |
| Il y a une faible compréhension des services commerciaux et de leur impact potentiel en cas de perturbation opérationnelle. La sensibilisation du conseil est limitée. | 6 |
| Nous n'avons pas une compréhension approfondie des services commerciaux importants et de leur impact. | 4 |
| Nous n'avons pas identifié ni documenté les services commerciaux importants. | 35 |

**Certains des commentaires formulés par les institutions :**

*« Les services commerciaux importants sont identifiés. Comme nous sommes toujours en cours d'exécution, toutes les tolérances n'ont pas été élaborées et approuvées par le conseil d'administration et la haute direction. »*

*« Les informations sont actuellement documentées au niveau des unités opérationnelles. Un projet est en cours pour centraliser les informations à des fins de résilience opérationnelle. Début des travaux prévu sous peu. »*

*« Nous identifions les processus au niveau des fonctions qui sont nécessaires pour fournir un service commercial de bout en bout. Une fois identifiées les fonctions sous-jacentes au sein d'un service métier, elles sont hiérarchisées à l'aide d'une approche basée sur les risques qui prend en compte le caractère critique du service et la disponibilité (…). »*

## **Q300-4** L’institution a-t-elle pris en compte toutes les parties de son activité et tous les services qu’elle fournit lors de l’identification des services commerciaux importants?

| Énoncés | Nombre de réponses |
|---|---|
| Toutes les parties de l'institution au Québec sont considérées dans l'identification des services aux entreprises. Cela a été clairement défini et s'inscrit dans notre structure organisationnelle. Par exemple, nous pouvons être en mesure de montrer comment nos activités sont structurées en fonction des fonctions économiques, des gammes d'activités ou de produits ou des segments d'utilisateurs finaux. Ceci est utilisé comme point de départ pour identifier les services commerciaux importants. | 135 |
| Lors de l'identification des services commerciaux importants, une attention est accordée à certains services soutenus par un plan crédible pour inclure tous les services. | 53 |
| Lors de l'identification des services commerciaux importants, une attention est accordée aux services, mais cela se fait de manière ad hoc et ne s'étend pas à tous les services. | 14 |
| L’attention est limitée dans l'institution et ne s’étend pas à tous les services. | 12 |
| Nous n'avons pas identifié ni documenté les services commerciaux importants. | 40 |

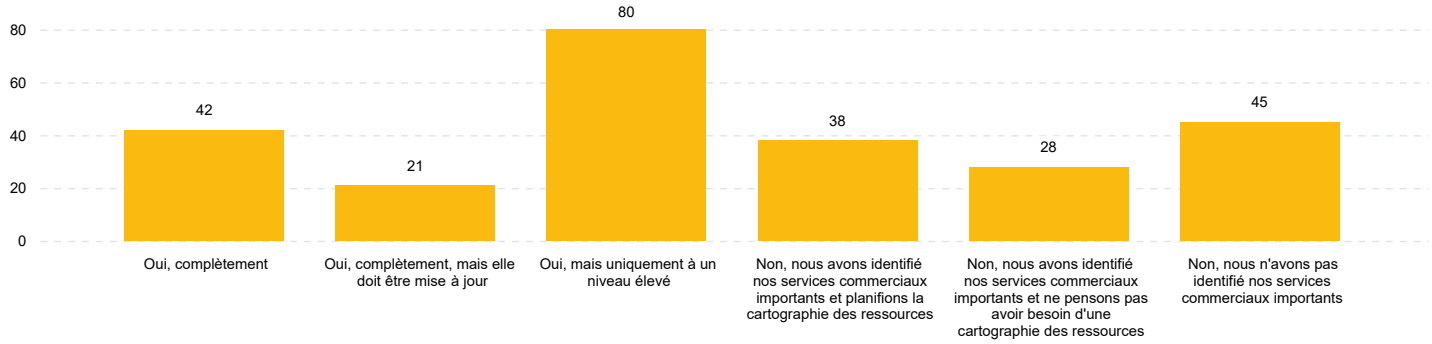
**Certains des commentaires formulés par les institutions :**

*« Bien que le terme "services commerciaux" ne soit pas utilisé, toutes les activités de chacun des secteurs d’activités ont été évaluées et leur tolérance d’interruption établie. »*

*« Les activités critiques ont été déterminées via la continuité des activités. En résilience, les services commerciaux importants seront identifiés. »*

*« Dans le contexte, la notion de "services commerciaux importants" tel que définie par l’AMF n’est pas observable au niveau de nos activités. »*

## **Q300-5** Votre institution a-t-elle déjà réalisé une cartographie des ressources des services commerciaux importants?




**Certains des commentaires formulés par les institutions :**

*« En tant que petite institution, la cartographie des ressources n'est pas un exercice nécessaire dans la mesure où les informations sont généralement connues de tous les dirigeants et peuvent être rapidement validées. »*

*« La cartographie des ressources est terminée pour tous les services métiers, mais pourrait être améliorée. »*

*« Pour le moment, nous continuons à identifier des services commerciaux critiques supplémentaires. »*

*« Les évaluations matérielles sont terminées ; Évaluations de l'impact sur les activités effectuées au niveau du secteur d'activité ; Ordre de récupération des systèmes déterminé par criticité. »*

## **Q300-6** Quelle est votre structure de gouvernance et de responsabilité pour l'identification, la fourniture et la maintenance de services commerciaux résilients?

| Énoncés | Nombre de réponses |
|---|---|
| Il existe une structure de gouvernance bien définie décrivant la responsabilité et la propriété des services commerciaux importants. Une propriété à jour des services commerciaux importants, des ressources de soutien et des interdépendances est maintenue et révisée. | 69 |
| La propriété des services commerciaux importants est documentée et inclut la propriété des ressources de soutien (facilitateurs). Le processus est dynamique et tout changement dans les services commerciaux et les ressources de soutien est reflété en temps opportun dans les responsabilités de propriété. | 75 |
| La propriété des services commerciaux importants et des ressources nécessaires est documentée, mais les ressources de soutien ne sont pas cartographiées et traitées de manière ad hoc. | 64 |
| La structure de gouvernance n'a pas été entièrement développée. Par conséquent, la responsabilité et la propriété des services commerciaux importants ne sont pas définies ou sont incomplètes. | 46 |

**Certains des commentaires formulés par les institutions :**

*« La structure même de l'organisation facilite l'identification des propriétaires des services commerciaux et l'identification des ressources nécessaires supportées par les données recueillies dans le cadre du programme de continuité des activités. »*

*« Avoir la bonne propriété, maintenir à jour la documentation et réévaluer la criticité, si quelque chose change - tout cela fait partie du plan visant à construire le programme de résilience opérationnelle. »*

*« Sur la base de la catégorisation décrite, la propriété est clairement articulée. La documentation des interdépendances entre les processus reste en cours de développement. »*

## **Q300-7** Comment vous assurez-vous que tous les services commerciaux, les ressources requises et les interdépendances ont été identifiés et que leur exhaustivité a été vérifiée?

| Énoncés | Nombre de réponses |
|---|---|
| Tous les services commerciaux, les ressources requises et les interdépendances sont identifiés et documentés. Il existe un processus pour capturer les changements dans l'institution et les refléter respectivement dans l'inventaire documenté des services commerciaux, des ressources requises et des interdépendances. | 71 |
| Tous les services commerciaux, les ressources requises et les interdépendances sont identifiés et documentés. Les modifications sont mises à jour et reflétées dans l'inventaire de manière ponctuelle. | 48 |
| Les services commerciaux, les ressources requises et les interdépendances sont identifiés pour les services commerciaux importants et documentés au cas par cas. | 97 |
| Aucun service commercial, ressource requise ou interdépendance n'est identifié ou documenté. Tout besoin de ressources est traité de manière réactive. | 38 |

**Certains des commentaires formulés par les institutions :**

*« Bien que le terme "services commerciaux" ne soit pas utilisé, toutes les interdépendances des activités critiques ont été documentées dans le cadre du programme de continuité des activités. »*

*« Les activités critiques ont été déterminées via la continuité des activités. En résilience, les services commerciaux importants seront identifiés. »*

*« Nous disposons d'un processus pour effectuer une évaluation annuelle des services commerciaux réalisés, ainsi que d'un processus ad hoc si un changement important est apporté, qui sont identifiés par le biais de processus normaux de projet ou de risque. »*

*« Nous avons mis en place des plans de continuité des activités qui sont actualisés chaque année (…) Il existe un processus de gestion des changements qui comprend l'identification des mises à jour pour le PCA et la reprise après sinistre. Cela n'a pas encore été fait pour tous les services commerciaux. »*

## **Q300-8** Comment identifiez-vous et classez-vous les services commerciaux critiques/importants, y compris les facteurs externes et internes à refléter en temps opportun dans les cotes de criticité? Ce processus intègre-t-il les besoins en ressources et les interdépendances?

| Énoncés | Nombre de réponses |
|---|---|
| Une évaluation de la criticité des services commerciaux identifiés, des ressources requises et des interdépendances est effectuée et documentée. Un processus est en place pour capturer les changements de criticité dus à des changements de facteurs internes ou externes, et les refléter respectivement dans l'inventaire documenté des services commerciaux, des ressources requises et des interdépendances. | 34 |
| L'évaluation de la criticité de tous les services commerciaux identifiés, des ressources requises et des interdépendances est effectuée et documentée. Des examens périodiques sont entrepris pour incorporer toutes les mises à jour/modifications afin de s'assurer que la liste est maintenue et à jour. | 107 |
| L'évaluation de la criticité des services commerciaux importants identifiés, des ressources requises et des interdépendances est effectuée et documentée, mais la liste n'est pas maintenue ou mise à jour. | 67 |
| Aucune évaluation de criticité n'est entreprise pour identifier les services commerciaux importants, les ressources nécessaires et les interdépendances. Les exigences sont évaluées et traitées de manière réactive. | 46 |

**Certains des commentaires formulés par les institutions :**

*« Il y a des évaluations de criticité en place pour des questions de continuité des affaires, de gestion de la relève et des incidents et ce, pour les plans de résolution et de recouvrement. Cet exercice n'a pas été complété dans le cadre de la résilience opérationnelle. »*

*« L'évaluation de la criticité est effectuée mais pas documentée. »*

*« Nous en sommes actuellement à notre premier cycle de pratique de résilience opérationnelle. Des révisions périodiques seront donc entreprises pour intégrer les mises à jour/changements dans les cycles futurs. »*

*« La criticité est évaluée (…) documentée pour tous les services métier identifiés et mise à jour au moins une fois par an. Des critères clairs ont été définis pour évaluer la criticité et les priorités de reprise. »*

## **Q300-9** Comment identifiez-vous les exigences de résilience pour vos services commerciaux les plus importants? Comment vous assurez-vous que les exigences sont examinées et tenues à jour?

| Énoncés | Nombre de réponses |
|---|---|
| Les exigences de résilience pour tous les services commerciaux importants sont identifiées et documentées. Un processus est en place pour saisir les changements dans les exigences dus à des changements de facteurs internes ou externes, et les refléter respectivement dans l'inventaire documenté des services commerciaux. | 46 |
| Les exigences de résilience pour tous les services commerciaux importants sont définies et documentées. Un inventaire à jour est maintenu et les exigences sont revues périodiquement et améliorées au besoin. | 69 |
| Des exigences de résilience ont été définies pour les services commerciaux importants. Un inventaire a été établi et revu au cas par cas. | 80 |
| Aucune exigence de résilience n'a été définie pour les services commerciaux importants. Le besoin d'un inventaire a été identifié et sera développé en temps voulu. | 59 |

**Certains des commentaires formulés par les institutions :**

*« Des exigences de résilience sont établies du côté des systèmes technologiques et dans la gestion des tiers les plus importants. »*

*« Nous identifions les besoins de résilience (en termes d'objectifs de temps de récupération) par secteur d'activité/fonction de service et mettons à jour les plans de continuité des activités au moins une fois par an. Nous effectuons l'exercice processus par processus par rapport au service métier de bout en bout. »*

*« Des critères clairs ont été définis pour évaluer la criticité de tous les processus opérationnels ainsi que les priorités et exigences de reprise (résilience). Tous les processus opérationnels sont examinés au moins une fois par an. Ce processus d'examen est géré par l'équipe de continuité des opérations. »*

## **Q300-10** Dans quelle mesure avez-vous complété l'inventaire de vos services commerciaux importants et de ses interdépendances?

| Énoncés | Nombre de réponses |
|---|---|
| L'inventaire des services commerciaux importants et des interdépendances est revu périodiquement et tenu à jour. Un processus est en place pour capturer et refléter les changements dans les dépendances internes ou externes. La liste et le processus souligné sont examinés de manière indépendante. | 71 |
| Un inventaire complet des services commerciaux importants et des interdépendances est maintenu, mais pas entièrement revu. Des outils appropriés sont en place pour saisir et refléter tout changement apporté à l'inventaire. | 56 |
| L'inventaire des services commerciaux et de leurs interdépendances est maintenu et inclut toutes les dépendances de tiers. Toute modification de l'inventaire est identifiée et documentée au cas par cas. | 69 |
| Il n'y a pas d'inventaire des services aux entreprises, des ressources nécessaires et des interdépendances. Toutes les exigences sont actuellement gérées par des unités commerciales individuelles et non consolidées dans un endroit central. | 58 |

**Certains des commentaires formulés par les institutions :**

*« Nous avons identifié les objectifs de temps de récupération, les dépendances et la criticité qui alimentent les exigences de résilience. »*

*« L'inventaire des dépendances aux tiers importants est effectué et maintenu au niveau des activités critiques des secteurs d'activités. »*

*« Le programme étant toujours en cours d'exécution, nous avons identifié les services commerciaux importants et nous sommes en bonne voie pour cartographier les interdépendances. Un processus est en place pour réévaluer tout changement significatif. »*

*« Nous disposons d'un inventaire de services importants, mais nous n'avons pas cartographié les interdépendances. »*

## **Q300-11** Comment vous assurez-vous que toutes les exigences de résilience pour vos services commerciaux les plus importants et leurs interdépendances ont été documentées et tenues à jour?

| Énoncés | Nombre de réponses |
|---|---|
| Les exigences de résilience ont été identifiées, classées et documentées pour tous les services commerciaux importants, y compris tous les facteurs externes et internes. La liste reflète les notes de criticité et est révisée périodiquement pour s'assurer qu'elle reste à jour. La liste intègre également les besoins en ressources et les interdépendances et fait l'objet d'un examen indépendant. | 48 |
| Les exigences de résilience ont été identifiées, classées et cartographiées dans tous les services commerciaux importants au niveau de l'unité d'affaire. Une liste consolidée des exigences est en cours d'élaboration afin de maintenir une source unique et d'assurer l'intégrité des exigences. En outre, la liste comprendra également la cote de criticité du service, les besoins en ressources et les interdépendances. | 95 |
| Les exigences de résilience ont été identifiées et classées au cas par cas pour tous les services commerciaux importants. Les exigences relatives à tous les facteurs externes et internes et à toutes les interdépendances ne sont pas pleinement prises en compte ou appliquées de manière cohérente. | 62 |
| Aucune exigence de résilience pour les services commerciaux ou les interdépendances n'est identifiée et documentée. Les exigences de résilience, y compris toutes les interdépendances, sont traitées de manière réactive. | 49 |

**Certains des commentaires formulés par les institutions :**

*« Nous avons défini des objectifs de temps de récupération dans le cadre de l'analyse d'impact sur l'activité, mais reconnaissons la nécessité d'un inventaire de toutes les exigences en matière de résilience opérationnelle. »*

*« Bien que nous ayons identifié et documenté des services commerciaux importants pour les entités juridiques dans d'autres pays, nous n'avons pas encore entrepris cette démarche au Canada. »*

## **Q300-12** En cas de perturbation opérationnelle, comment préparez-vous et priorisez-vous vos ressources et actions afin d'assurer la continuité de vos services commerciaux et de minimiser les dommages aux consommateurs/ clients?

| Énoncés | Nombre de réponses |
|---|---|
| Processus en place pour capturer les quasi-accidents, les leçons apprises et alimenter les processus de test et d'évaluation. L'analyse de l'horizon est intégrée pour identifier et se préparer aux événements potentiels dans le cadre des affaires comme d'habitude. Le processus de continuité des activités est mûri et entièrement intégré dans toute l'organisation avec la participation de la haute direction. Des tests inopinés sont effectués pour tester le cadre de continuité des activités. Le cadre de continuité des activités est testé périodiquement pour évaluer son efficacité. | 42 |
| Un processus intégré de détection et de notification avec d'autres parties prenantes clés et des tiers est en place et testé périodiquement. Les arrangements et les tests de récupération de données incluent des scénarios informés par des incidents passés, des informations de gestion et des dépendances de tiers. Un cadre de continuité des activités en place pour garantir qu'une réponse coordonnée peut être fournie lors d'un incident opérationnel. Des simulations sont effectuées périodiquement avec les parties prenantes concernées, y compris la haute direction. | 100 |
| En cas d'interruption opérationnelle, les modalités de récupération des données et les exigences de test sont déterminées par l'institution et incluent les fournisseurs de services (y compris les fournisseurs de services tiers) avec des métriques et/ou des cadres pertinents définis. Un cadre de continuité des activités est en place pour assurer une réponse coordonnée lors d'une perturbation opérationnelle. Des simulations sont réalisées ponctuellement pour tester le cadre de continuité d'activité. | 107 |
| En cas de perturbation opérationnelle, les modalités de reprise du service ne sont pas déterminées ou sont déterminées isolément. Par ex., le service informatique détermine les actions sans aucune intervention de l'institution. La réponse pour assurer toute continuité lors d'une perturbation opérationnelle est ad hoc. | 5 |

**Certains des commentaires formulés par les institutions :**

*« Nous nous servons des quasi-accidents ou d'incidents, comme la pandémie, pour tester le cadre de continuité des activités plutôt que de procéder par simulations pour l'instant étant donné notre petite taille. »*

*« Les tests sont pour le moment "annoncés", mais les participants au test ne sont pas au courant du type de scénario de perturbation (…) avons organisé des exercices non annoncés dans le passé et nous chercherons à les mettre en œuvre dans un avenir proche. »*

*« Des tests sont effectués périodiquement. Des exercices de coaching en cas de violation sont également effectués périodiquement. Des tests de reprise après sinistre sont effectués chaque année sur les systèmes et réseaux critiques. »*

## **Q300-13** Quelle est votre approche de test et à quelle fréquence vos plans de continuité sont-ils testés pour garantir que vos services commerciaux restent efficaces et adaptés à leur objectif?

| Énoncés | Nombre de réponses |
|---|---|
| Les plans de test incluent des scénarios qui prennent en compte les problèmes systémiques et environnementaux affectant plusieurs services commerciaux. Les incidents de courte et de longue durée qui ont un impact sur les services commerciaux sont évalués dans les plans de test. Les plans sont testés périodiquement et mis à jour pour refléter tout changement. | 53 |
| L'approche de test est bien définie et régie par des politiques et des procédures établies. Les plans et scénarios de tests facilitent la prise de décision et couvrent les services commerciaux dans leur ensemble, y compris les tiers. Les plans de test prévoient des ressources flexibles pour assurer la continuité des services prioritaires afin de minimiser les interruptions d'activité et les dommages aux consommateurs en fonction de l'impact et de la durée de l'incident/plan de test, selon les besoins. Les tests de continuité sont effectués conformément au calendrier et les leçons apprises/améliorations sont incorporées dans les plans de test. | 61 |
| L'approche de test est bien définie et régie par des politiques et des procédures établies. L'approche de test définit la fréquence des tests, les types de tests, l'utilisation d'exercices, etc. et est limitée à des plates-formes ou des systèmes individuels. Les tests de continuité sont effectués conformément au calendrier et le résultat du test est enregistré à des fins de transparence. | 110 |
| L'approche de test n'est pas entièrement développée et est appliquée de manière ad hoc. Les tests de continuité ne sont pas effectués et la réponse à un incident opérationnel est purement réactive. | 30 |

**Certains des commentaires formulés par les institutions :**

*« L'évaluation et les tests des tiers constituent un domaine d'attention et d'amélioration continue. »*

*« Les tests sont effectués tout au long de l'année pour les systèmes identifiés comme critiques. Les scripts de test sont mis à jour chaque année en fonction des processus critiques identifiés dans chaque plan de continuité des activités. Les leçons apprises sont enregistrées après chaque test et intégrées aux futurs plans de test. »*

*« Nous organisons chaque année un événement de simulation de catastrophe. L'événement de catastrophe varie d'une année à l'autre (…) sélectionner des événements qui auront un impact sur plusieurs scénarios de catastrophe (lieu de travail, main-d'œuvre, informatique/technologie, fournisseur) et services. »*

*« Les tests n'ont pas encore été effectués car le déploiement de la résilience est en cours de développement en attendant les normes (…). »*

## **Q300-14** À quelle fréquence testez-vous vos capacités de réponse et de récupération pour différents scénarios perturbateurs?

## **Q300-15** Quels plans et systèmes de communication (pour les parties prenantes internes et externes) avez-vous mis en place pour faire face aux perturbations opérationnelles?

| Énoncés | Nombre de réponses |
|---|---|
| Des systèmes automatisés/arborescences d'appels et des plans de communication sont en place pour contacter tout le personnel lors d'un incident, et cela est maintenu et cohérent tout au long de toute perturbation. Le protocole de communication est périodiquement revu et testé pour intégrer les fournisseurs de services, les partenaires, les clients et les leçons apprises incorporées. | 80 |
| Les plans de communication incluent toutes les informations pertinentes pour permettre une stratégie de communication coordonnée pour les différents canaux de communication/parties prenantes. Les plans comprennent des lignes d'attente/modèles prédéterminés pour les communications et sont périodiquement testés pour l'efficacité et les améliorations apportées dans le cadre des leçons apprises. Les plans incluent également des détails sur les fournisseurs de services externes, les partenaires et les bénéficiaires de services pour garantir que toute interdépendance est traitée en temps opportun afin de minimiser les perturbations. | 57 |
| Outils/mécanismes en place pour mettre à jour les informations de contact sur une base périodique. Les cascades d'appels sont appelées en temps opportun lors d'un incident. Toutes les communications avec les parties prenantes et les clients sont intégrées dans le cadre du plan de communication de crise et sont alignées sur un chemin d'escalade convenu. Les plans incluent également des détails sur les fournisseurs de services externes, les partenaires et les bénéficiaires de services pour garantir que toutes les interdépendances sont traitées en temps opportun afin de minimiser les perturbations. | 110 |
| Il n'y a pas de plan de communication formel en dentelle pour s'adresser aux parties prenantes externes. Comme pour les parties prenantes internes, les coordonnées sont enregistrées mais non tenues à jour et toute cascade de communication est gérée de manière informelle. | 7 |

**Certains des commentaires formulés par les institutions :**

*« La taille de l'entreprise permet d'assurer la coordination de toutes les parties prenantes et de rester en contact avec la haute direction et le personnel clé de l'organisation, ce qui lui permet de réagir rapidement aux situations de crise. »*

*« Nous gérons la communication interne avec nos collaborateurs via un système de communication de masse, régulièrement utilisé et testé, tandis que les contacts commerciaux (prestataires de services, tiers, clients) sont contactés via des procédures de communication commerciale établies. »*

## **Q300-16** Comment obtenez-vous l'assurance qu'un événement/perturbation opérationnelle a été récupéré de manière satisfaisante et que le service normal a repris?

| Énoncés | Nombre de réponses |
|---|---|
| Stratégie de récupération et approche de test en place pour couvrir la reprise après sinistre de bout en bout pour les services commerciaux ainsi que pour couvrir une gamme de scénarios environnementaux, externes et géopolitiques. Des tiers sont inclus dans les scénarios de test. Une analyse des causes profondes est effectuée sur toutes les perturbations, le conseil d'administration et la haute direction supervisant toute mesure corrective. Les plans sont examinés de manière indépendante par la 3e ligne de défense. | 38 |
| La résilience est intégrée et la stratégie de reprise alignée sur les besoins de l'institution pris en charge par l'infrastructure, par ex. sauvegardes de réplication fréquentes et planifiées sur et hors site. Les copies papier des plans sont conservées hors site où elles peuvent être consultées en toute sécurité. Un processus de support fournisseur efficace avec des SLA est en place et les contrats sont évalués de manière cohérente, en particulier lorsque la récupération du service commercial dépend uniquement de tiers. Les tests de reprise après sinistre des services aux entreprises sont effectués à travers des scénarios graves mais plausibles, c'est-à-dire que l'entreprise et le tiers sont testés ensemble. | 84 |
| Contrôles physiques et infrastructure technique en place pour permettre la reprise des services commerciaux. Le processus de récupération suit des contrôles définis qui sont reproductibles et alignés sur les politiques et les plans. S'il dépend d'un soutien externe, le recouvrement est limité aux contrats en place. Définition des objectifs de temps de récupération (RTO) pour les applications principales et récupération globale du service commercial en place. Les centres de données sont construits à cet effet et respectent les normes de l'industrie. | 125 |
| Il n'y a pas de procédures formelles en place pour assurer la reprise des affaires comme d'habitude après une perturbation opérationnelle. La reprise des affaires comme d'habitude est gérée de manière ad hoc et ne suit pas les contrôles définis, n'est alignée sur aucun plan et ne correspond pas aux accords de niveau de service convenus. | 7 |

**Certains des commentaires formulés par les institutions :**

*« Nous en obtenons l'assurance avec une analyse des causes profondes après l'événement, en prenant en compte les éléments importants. »*

*« Nous n'avons jamais eu de perturbation majeure. »*

*« Au niveau de l'entreprise, la gravité de la perturbation détermine le niveau de gestion avec lequel l'analyse des causes profondes est partagée. »*

*« Le suivi des incidents significatifs/perturbations opérationnelles est documenté et validé par les unités commerciales dans le cadre du processus d'évaluation post-événement. Il s'agit d'un domaine d'amélioration continue. »*

## **Q300-17** Veuillez sélectionner l’approche la plus appropriée pour vos examens post-incident.

| Énoncés | Nombre de réponses |
|---|---|
| L'examen post-incident inclut (ou fait référence à) l'examen post-incident ou l'analyse d'incident du fournisseur. Des enseignements clairs et efficaces ont été réinjectés dans les domaines pertinents. Analyse des causes profondes entreprise pour toutes les pannes opérationnelles ayant un impact sur les services commerciaux. Le conseil d'administration et les membres supérieurs supervisent toutes les mesures correctives. Dans le cadre de l'amélioration continue, les leçons apprises sont intégrées dans les documents de planification de la résilience opérationnelle. | 51 |
| Un processus formel d'examen post-incident est en place. Le processus définit les étapes à suivre pendant et après une perturbation opérationnelle. La documentation sur les incidents, y compris les données des tickets, les délais et l'analyse des causes profondes, est remplie pour toutes les perturbations pendant et après l'incident. Les informations sur les tendances sont renseignées et permettent à la haute direction de prendre des décisions éclairées. La cause profonde est entreprise et les leçons apprises sont incorporées dans les plans de test pour l'exhaustivité. | 91 |
| Un processus formel d'examen post-incident est en place. Le processus définit les étapes à suivre suite à une perturbation opérationnelle. L'examen post-incident est compilé avec des informations rassemblées après (plutôt que pendant) l'incident. Les actions sont convenues et corrigées conformément à l'examen post-incident. Les informations sur les tendances sont renseignées au cas par cas. L'analyse des causes profondes est entreprise de manière ad hoc et, le cas échéant, les plans de test sont mis à jour pour intégrer les leçons apprises. | 82 |
| Il n'y a pas de politique/processus formel d'examen post-incident en place. L'examen est effectué de manière informelle pour toute perturbation opérationnelle. Les enseignements tirés de l'incident sont mis à jour/intégrés dans le cadre du plan de test. | 30 |

## **Q300-18** Comment recherchez-vous l'assurance et validez-vous l'efficacité des plans de reprise après sinistre et de continuité des services commerciaux, en particulier lorsque les services sont fournis par un fournisseur tiers?

| Énoncés | Nombre de réponses |
|---|---|
| L'entraînement aux incidents ou l'exercice de jeu de guerre est effectué sur une base périodique et comprend toutes les facettes du plan. Les exercices comprennent des simulations inopinées et couvrent un éventail complet de types de tests et de services commerciaux (de bureau à bout en bout, y compris les parties externes, etc.). Les *playbooks* sont testés en interne avec des tiers et des fournisseurs et assurés indépendamment par la 3e ligne de défense. En ce qui concerne les tests de reprise après sinistre, les tests de sauvegarde et de récupération évaluent que les points de défaillance uniques, les objectifs de point de récupération sont définis et atténués et, dans le cas contraire, le risque a été accepté. Les tiers sont pleinement impliqués dans la planification et les tests de bout en bout des services commerciaux importants. | 8 |
| Les plans de test sont alignés sur les objectifs clés et l'appétit pour les risques et ceux-ci sont testés périodiquement. Les leçons apprises sont incorporées et traitées dans le cadre de la documentation mise à jour pour les exigences de planification de la continuité des activités. Le programme régulier d'exercices comprend une variété de différents types de scénarios réalistes (bureau, simulation, etc.). Les exercices incluent une variété d'intervenants primaires et secondaires. Le programme d'assurance comprend une vérification et une validation indépendantes (3e ligne de défense) des plans et des tests. Les tiers qui prennent en charge des services commerciaux importants sont pris en compte et inclus dans les tests. | 57 |
| Un calendrier formel d'exercices pour former et répéter le plan de continuité des activités et la capacité de gestion de crise existe. L'exercice comprend la réalisation d'examens de bureau pour tester les intervenants principaux et/ou secondaires. Les plans de test sont liés aux objectifs et aux risques de continuité des services commerciaux. Le programme d'assurance (1re ligne de défense) comprend la vérification et la validation des plans et des tests. Les tierces parties sont considérées comme faisant partie du processus de planification mais ne sont pas impliquées dans les tests. | 131 |
| Aucune assurance formelle n'est entreprise pour valider l'efficacité des plans de reprise après sinistre et de continuité des services pris en charge par des tiers. Au lieu de cela, la confiance est placée sur le tiers pour fournir un service continu (conformément à l'accord de niveau de service) et informer l'entreprise de toute lacune. Les tiers ne sont inclus dans aucun exercice ou simulation de crise. | 58 |

## **Q300-19** Avez-vous collaboré avec des tiers critiques pour comprendre le risque potentiel de contagion et pris des mesures pour vous assurer que les activités de rétablissement sont clairement comprises par les deux parties?

| Énoncés | Nombre de réponses |
|---|---|
| Les modalités de recouvrement sont bien définies et intégrées dans l'ensemble de l'organisation. La planification prend en compte les dépendances tierces critiques et leurs capacités de récupération. Les fournisseurs tiers sont impliqués dans l'élaboration de plans/scénarios de test qui prennent en compte les impacts systémiques et environnementaux pour comprendre et atténuer tout risque de contagion pour les services commerciaux importants. | 17 |
| Les accords de récupération impliquent des scénarios détaillés pour tous les services commerciaux critiques/importants informés par les incidents passés, les informations de gestion et les dépendances de tiers. Les tests sont effectués conjointement par les deux parties et comprennent la validation des principales dépendances pour comprendre le risque potentiel de contagion. | 26 |
| Les plans de récupération sont définis par l,institution et basés sur l'identification des services commerciaux critiques/importants et leur dépendance vis-à-vis des fournisseurs de services tiers. Les tests sont effectués sur une base ad hoc et se limitent aux tests au niveau des composants. | 183 |
| Les accords de récupération ne sont pas déterminés ou sont déterminés de manière isolée et ne tiennent pas compte des services fournis par des tiers. | 28 |

**Certains des commentaires formulés par les institutions :**

*« Certains fournisseurs de services tiers ne peuvent être testés (i.e.; Microsoft, Bell, Vidéotron, etc.). »*

*« Comme toutes les interdépendances des services commerciaux importants n'ont pas été prises en compte, nous exigeons actuellement des stratégies de sortie uniquement pour les fournisseurs les plus critiques. »*

*« Les fournisseurs jugés critiques sont invités à fournir leur plan de continuité des activités conformément à la politique au moment de l'évaluation de la sécurité des informations des tiers, qui est examiné par notre CISO. »*

## **Q300-20** Comment comptez-vous utiliser la cartographie des services commerciaux importants dans votre approche de test?

| Énoncés | Nombre de réponses |
|---|---|
| Nous pouvons démontrer comment nous utiliserons l'outil de cartographie pour faciliter les tests. Par exemple, nous utiliserons notre cartographie pour aider à concevoir des scénarios sévères mais plausibles, augmenter ou diminuer la gravité des scénarios, etc. Notre planification des tests prend en compte l'ensemble de la chaîne d'activités qui sous-tendent le service commercial important, tiré des données de cartographie. Nous pouvons démontrer comment notre approche de test fournira une couverture appropriée sur les ressources qui prennent en charge la prestation du service, y compris les tiers qui prennent en charge la prestation des services commerciaux importants. | 24 |
| Nous avons des plans en place pour examiner et tester pleinement les activités de bout en bout qui sous-tendent les services commerciaux importants. Les plans de test prennent en compte et incluent les activités qui sous-tendent les services commerciaux importants, tirés des données de cartographie. Nous envisageons d'étendre cela pour inclure d'autres ressources, y compris des tiers critiques qui prennent en charge la fourniture des services commerciaux importants. | 76 |
| Nous avons une bonne compréhension des données de cartographie des services commerciaux importants et prévoyons de les inclure dans notre approche globale de test. Nous développons des plans de test qui prendront pleinement en compte et testeront les activités de bout en bout qui sous-tendent les services commerciaux importants. | 112 |
| Notre plan de test ne prend pas en compte et/ou n'inclut pas les données de cartographie des services commerciaux importants. Nous n'avons pas encore de plans en place pour résoudre ce problème. | 42 |

**Certains des commentaires formulés par les institutions :**

*« Nous exploitons l'importante cartographie des services métiers dans le développement et l'exécution de nos exercices de scénarios de perturbations graves mais plausibles. Nous continuerons à étendre nos exercices pour les rendre plus complexes et refléter les perturbations émergentes. »*

*« Le programme de résilience opérationnelle n'a été mis en place que récemment et n'a pas encore défini les services commerciaux importants et les cartographies associées. »*

## **Q300-21** Quel type de tests avez-vous l'intention d'utiliser et fourniront-ils une assurance suffisante de l'efficacité de la capacité de réponse et de récupération de votre institution?

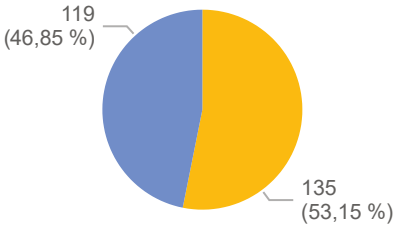
| Énoncés | Nombre de réponses |
|---|---|
| Nos plans de test couvrent les niveaux d'assurance obtenus à partir du type de tests de scénarios - cela peut inclure des évaluations sur papier (assurance inférieure), des simulations (assurance moyenne) ou des tests de systèmes en direct (assurance élevée). Test de nos plans de récupération pour les scénarios de disponibilité (par exemple, pannes de système) et d'intégrité (par exemple, corruption ou perte de données), proportionnés à notre taille et à notre complexité et tenant compte des vulnérabilités, par exemple, adoption de nouvelles technologies/*cloud*. L'approche de test est examinée et approuvée par un organe de gouvernance approprié pour s'assurer qu'il fournit une assurance suffisante sur l'efficacité de ses capacités d'intervention et de récupération. | 77 |
| Notre plan de test est basé sur et lié à la cartographie de nos services commerciaux importants. Les données de cartographie et les activités soulignées sont mises à jour et approuvées par les forums de gouvernance appropriés. Nous avons clairement défini l'inclusion de tiers dans le cadre de notre approche de test. | 99 |
| Les données de test sont basées sur et liées à la cartographie de nos services commerciaux importants, cependant, les données ne sont pas régulièrement mises à jour et maintenues de manière ad hoc. Nous n'avons pas envisagé la manière dont les tiers seront inclus dans la portée des tests. L'approche de test n'est pas revue régulièrement. | 67 |
| Nous utilisons des données de cartographie obsolètes/inexactes pour nos tests (c'est-à-dire non basées sur une cartographie des services commerciaux importants), ce qui ne fournit aucune assurance sur la couverture des services commerciaux importants. | 11 |

## **Q300-22** Quels problèmes de tiers ou d'externalisation votre institution financière a-t-elle rencontrés, le cas échéant?

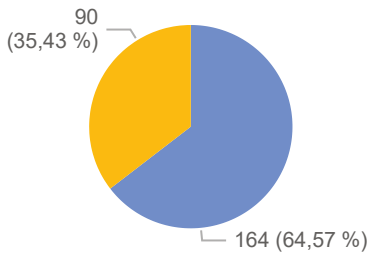
| Énoncés | Nombre de réponses |
|---|---|
| Problèmes informatiques | 119 |
| Interruption de service | 164 |
| Manque de surveillance | 43 |
| Exécution contractuelle | 88 |
| Sécurité des données | 103 |
| Problèmes de sous-traitance | 50 |
| Assistance du fournisseur | 60 |

**Légende** Oui Non

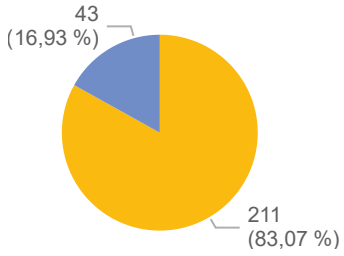
Problèmes informatiques



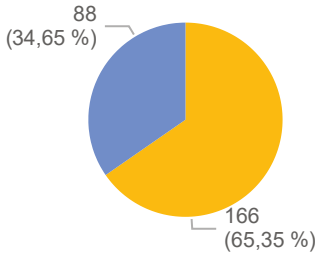

Interruption de service



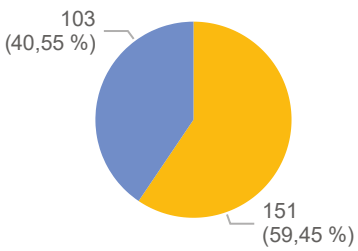

Manque de surveillance



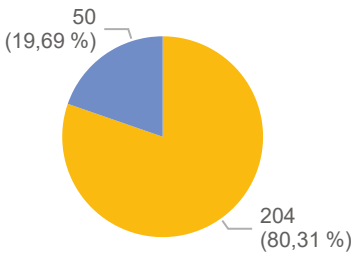

Exécution contractuelle



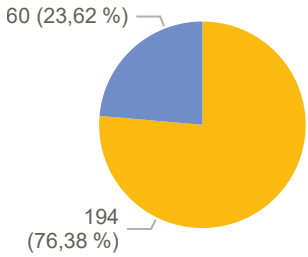

Sécurité des données




Problèmes de sous-traitance




Assistance du fournisseur



## **Q300-23** Comment identifiez-vous votre dépendance vis-à-vis des services fournis par des tiers (y compris les intra-affiliés) pour la fourniture de services commerciaux importants qui pourraient entraîner un préjudice pour le client?

| Énoncés | Nombre de réponses |
|---|---|
| Les tierces parties et les dépendances associées ont été identifiées et les stratégies d'atténuation documentées pour assurer la continuité des services à travers les services commerciaux importants. Le registre des tiers est examiné de manière indépendante, par exemple par la 3e ligne de défense sur une base périodique et les problèmes sont transmis, le cas échéant, à la haute direction et/ou au conseil d'administration. | 63 |
| Les tierces parties et les dépendances associées ont été identifiées et les stratégies d'atténuation documentées pour assurer la continuité du service à travers les services commerciaux importants. Le registre des tierces parties comprend quelques 4e parties et est tenu à jour périodiquement. Les exceptions sont signalées à la haute direction et/ou au conseil d'administration via les informations de gestion appropriées. Aucun examen indépendant n'est effectué pour valider la liste. | 33 |
| Les tierces parties ont été identifiées et classées en fonction de leur importance pour la fourniture des services commerciaux importants qu'elles prennent en charge. Les interdépendances sont cartographiées et documentées dans un registre de tiers et comprend une liste des tiers concernés. Le risque de concentration n'est pas entièrement compris/ cartographié. Le niveau d'engagement est proportionnel à la criticité du fournisseur. | 112 |
| Il n'y a pas de vue formellement documentée des fournisseurs tiers critiques. Les tierces parties sont répertoriées de manière ad hoc et identifiées en fonction de leur matérialité (valeur financière) et de la criticité des services qu'elles soutiennent. | 46 |

**Certains des commentaires formulés par les institutions :**

*« L'intégration de la gestion des risques liés aux tiers est actuellement une lacune que l'organisation cherche à atténuer (…). »*

*« Les dépendances vis-à-vis de tiers sont identifiées dans l'inventaire des tiers ainsi que dans les évaluations d'impact et les plans de continuité (…) tiers utilisés pour plusieurs services métier sont partiellement identifiés (…) risque de concentration n'a pas été entièrement évalué. »*

*« Le registre des tiers n'inclut pas de liste des quatrièmes parties concernés. »*

## **Q300-24** Comment effectuez-vous une diligence raisonnable (à la fois opérationnelle et financière) sur les accords tiers nouveaux et existants pour évaluer et gérer les risques et les vulnérabilités qu'un tiers peut introduire dans votre environnement d'exploitation?

| Énoncés | Nombre de réponses |
|---|---|
| Le processus et les contrôles de diligence raisonnable ont fait l'objet d'un examen indépendant périodique et les sujets de préoccupation sont transmis, le cas échéant, à la haute direction et/ou au conseil d'administration. Les exceptions à la diligence raisonnable des tiers sont transmises à la haute direction et/ou au conseil d'administration via des informations de gestion appropriées. | 53 |
| Une diligence raisonnable est périodiquement effectuée sur des tiers nouveaux et existants pour évaluer et gérer les risques et les vulnérabilités qu'un tiers peut introduire dans l'environnement d'exploitation. Les exceptions à la diligence raisonnable des tiers sont transmises à la haute direction et/ou au conseil d'administration via des informations de gestion appropriées. La diligence raisonnable couvre une gamme de domaines technologiques ainsi que l'adéquation des ressources et devrait prévoir différents risques opérationnels dans le cadre d'arrangements tels que les données sensibles, la fourniture de services *cloud* sur mesure et les services standard, la concentration et les considérations à l'étranger. | 66 |
| Une diligence raisonnable est périodiquement effectuée sur des tiers nouveaux et existants pour évaluer et gérer les risques et les vulnérabilités qu'un tiers peut introduire dans l'environnement d'exploitation. La diligence raisonnable prend en compte les risques associés à la capacité du tiers à fournir un service continu pour tous les services commerciaux importants et tout conflit d'intérêts potentiel et sa résilience financière. La rigueur du processus de diligence raisonnable est proportionnelle à la nature, à l'ampleur et à la complexité de l'arrangement avec un tiers. | 128 |
| Aucune diligence raisonnable formelle n'est effectuée pour les fournisseurs tiers nouveaux ou existants. | 7 |

## **Q300-25** Quelle est la nature/le niveau des droits de résiliation (la possibilité de mettre fin formellement à un contrat) et comment votre plan de sortie prend-il en compte les obligations réglementaires minimales?

| Énoncés | Nombre de réponses |
|---|---|
| Les droits de résiliation sont documentés et validés. Les preuves documentées des plans de sortie de tiers sont également conservées, validées et examinées de manière indépendante, y compris la conformité aux dispositions réglementaires. Les plans de sortie prennent également en compte : a) période minimale pour exécuter une disposition de résiliation, b) dispositions pour faciliter la transférabilité des services à une institution-relais ou à un autre tiers (ou une alternative équivalente). | 63 |
| Les contrats de sortie avec des tiers incluent des droits de résiliation en cas de rupture du contrat. Par exemple, si la contrepartie ne respecte pas systématiquement les niveaux de service convenus, l'institution est en mesure de mettre fin à l'accord et de ramener le service en interne ou de le transférer à un autre fournisseur de services tiers. Les délais sont mutuellement convenus et mis en œuvre. | 142 |
| Les droits de résiliation et les stratégies de sortie appropriées ne sont pas entièrement développés pour tous les accords de service tiers critiques. Des plans de sortie sont en cours d'élaboration et seront inclus dans l'entente contractuelle. | 40 |
| Il n'existe aucun plan de sortie formel. Les relations avec les tiers sont gérées d'un commun accord et ne sont pas exécutoires par la loi. | 9 |

**Certains des commentaires formulés par les institutions :**

*« Des stratégies de sortie formelles sont élaborées, approuvées par la haute direction et révisées périodiquement pour tous les tiers importants/critiques. »*

*« Les fournisseurs critiques disposent de dispositions plus solides en matière de résiliation et d'une analyse plus approfondie des stratégies/scénarios de sortie. »*

## **Q300-26** Connaissez-vous les services fournis par les tiers et leurs fournisseurs?

| Énoncés | Nombre de réponses |
|---|---|
| Un registre précis est tenu de tous les services fournis par les tiers. Des processus et des procédures sont en place pour s'assurer que les nouveaux tiers et/ou les changements apportés aux services existants sont saisis dans le registre. La liste est validée périodiquement et révisée de manière indépendante par la 3e ligne de défense. | 49 |
| Un registre est tenu de tous les fournisseurs tiers critiques et des services qu'ils fournissent. Le risque de concentration chez tous les fournisseurs critiques a été identifié et des stratégies d'atténuation documentées. Le niveau d'engagement est proportionnel à la criticité du fournisseur. Des processus et des procédures sont en place pour s'assurer que les nouveaux tiers critiques et/ou les changements apportés aux services existants fournis sont saisis dans le registre. | 120 |
| Une liste est tenue des fournisseurs tiers critiques et des services qu'ils fournissent et maintenus sur une base ad hoc. Le risque de concentration chez tous les fournisseurs critiques n'est pas entièrement compris et est en cours de cartographie. | 72 |
| Il n'y a pas de liste centralisée des fournisseurs et services tiers. Les unités commerciales sont chargées de gérer les relations individuelles. Le risque de concentration n'est pas pris en compte. | 13 |

## **Q300-27** Avez-vous mis en place des processus et des procédures efficaces pour évaluer les risques et les capacités de résilience opérationnelle de vos fournisseurs de services tiers?

| Énoncés | Nombre de réponses |
|---|---|
| Les fournisseurs tiers et leur prestation de services sont évalués en fonction de leur impact potentiel sur la prestation des services commerciaux importants d'une entreprise et intégrés dans tout scénario de test ou exercice. Les informations de gestion pertinentes sont partagées avec le conseil d'administration pour aider à prendre des décisions éclairées et toutes les conclusions sont enregistrées et mises en œuvre. | 71 |
| Les risques de résilience opérationnelle de tous les fournisseurs tiers critiques sont examinés conformément à la politique, mais sur une base ad hoc. | 129 |
| Tous les tiers critiques ne sont examinés qu'une seule fois, à l'étape de l'intégration et en fonction des risques qu'ils représentent. Les découvertes sont enregistrées. Aucun autre examen n'est effectué tout au long du cycle de vie. | 38 |
| Aucune évaluation des fournisseurs tiers n'est entreprise spécifiquement par rapport aux risques qu'ils représentent. | 16 |

Sans frais : 1 877 525-0337
lautorite.qc.ca

**Québec**
418 525-0337
Place de la Cité, tour PwC
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

**Montréal**
514 395-0337
800, rue du Square-Victoria, bureau 2200
Montréal (Québec) H3C 0B4