Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA sur la surveillance 05/2025

Résilience opérationnelle chez les banques, les personnes selon l'art. 1*b* LB, les maisons de titres et les infrastructures des marchés financiers

10 novembre 2025

Laupenstrasse 27, 3003 Berne, Tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

1 Introduction

Les banques, les personnes visées à l'art. 1*b* de la loi fédérale du 8 novembre 1934 sur les banques (LB ; RS *952.0*), les maisons de titres et les infrastructures des marchés financiers sont tenues de mettre en œuvre une gestion des risques adéquate dans le cadre de leurs activités. Cette gestion des risques doit couvrir l'ensemble des activités et être organisée de façon à ce que les risques principaux puissent être détectés, évalués, gérés et surveillés. Dans un contexte marqué par l'augmentation de divers risques sur les marchés financiers et par de nouveaux défis opérationnels (notamment les cyberattaques), la FINMA accorde depuis longtemps une attention particulière non seulement aux risques opérationnels en général, mais également à la résilience opérationnelle des établissements.

La résilience opérationnelle désigne la capacité de l'établissement à rétablir ses fonctions critiques en cas d'interruptions dans les limites de la tolérance aux interruptions. Il s'agit autrement dit de la capacité de l'établissement à identifier les menaces et les défaillances éventuelles, à s'en protéger et à y réagir, à rétablir la marche ordinaire des affaires en cas d'interruptions et à réduire au minimum les conséquences sur l'exécution des fonctions critiques. La résilience opérationnelle diminue non seulement les risques résiduels d'interruptions, mais aussi le risque inhérent de subir une interruption.

Le secteur financier est aujourd'hui fortement interconnecté et interdépendant, ce qui se traduit par une concentration des risques. Une perturbation dans un domaine peut avoir d'importantes répercussions sur d'autres parties du système financier. La résilience opérationnelle est donc essentielle pour assurer le bon fonctionnement des marchés financiers. Ainsi, en mettant l'accent sur la résilience opérationnelle des établissements financiers, la FINMA renforce non seulement la protection des créanciers, mais également le bon fonctionnement des marchés financiers en tant que tels, ce qui est primordial pour assurer la solidité du système financier.

La présente communication sur la surveillance repose sur les résultats d'une enquête réalisée par la FINMA auprès de 267 banques, maisons de titres, groupes financiers et infrastructures des marchés financiers (ci-après : les établissements) sur les moyens qu'ils mettent en œuvre pour garantir leur résilience opérationnelle, avec pour date de référence le 31 décembre 2024.

Le but de la présente communication sur la surveillance est de sensibiliser à la question de la résilience opérationnelle et de ce fait la mise en œuvre effective des différentes exigences prudentielles ainsi que le renforcement ciblé de la résilience opérationnelle face aux menaces croissantes et aux chocs opérationnels.

2 Bases légales

Pour les banques et les personnes visées à l'art. 1*b* LB, l'obligation d'identifier, de limiter et de surveiller leurs risques découle principalement des exigences organisationnelles selon les art. 1*a*, 1*b*, 3 al. 2 let. a et 3*c* LB en relation avec les art. 12 al. 2 et 14*e* de l'ordonnance du 30 avril 2014 sur les banques (OB ; RS *952.02*).

Pour les maisons de titres, cette obligation découle pour l'essentiel des art. 9 al. 2, 41 et 49 de la loi fédérale du 15 juin 2018 sur les établissements financiers (LEFin ; RS *954.1*) ainsi que des art. 12 al. 4 et 68 de l'ordonnance du 6 novembre 2019 sur les établissements financiers (OEFin ; RS *954.11*). Enfin, pour les infrastructures des marchés financiers, elle découle de l'art. 8 al. 3 de la loi du 19 juin 2015 sur l'infrastructure des marchés financiers (LIMF ; RS *958.1*) et de l'art. 9 al. 1 let. d de l'ordonnance du 25 novembre 2015 sur l'infrastructure des marchés financiers (OIMF ; RS *958.11*).

La FINMA a précisé sa pratique de surveillance relative à cette obligation dans sa circulaire 2023/1 « Risques et résilience opérationnels – banques ».

3 Enseignements tirés de l'enquête

Les 267 établissements interrogés par la FINMA ont évalué la maturité de leur propre résilience opérationnelle à hauteur de 7,5 (valeur moyenne) et celle du secteur financier suisse dans son ensemble à hauteur de 6,7 (valeur moyenne) sur une échelle de 0 à 10[1]. Les principaux enseignements tirés de l'enquête sur la garantie de la résilience opérationnelle sont présentés ci-après.

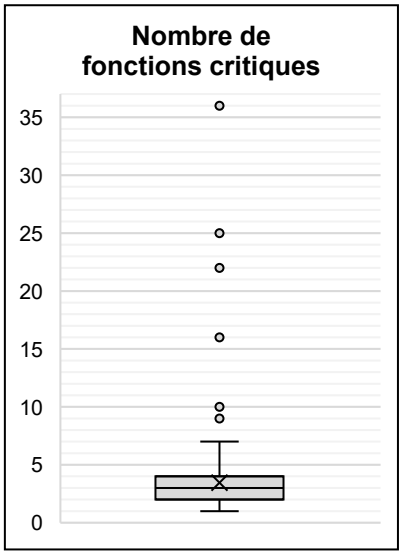
3.1 Fonctions critiques[2]

Enseignements

Le graphique ci-dessous présente sous forme agrégée le nombre de fonctions critiques définies par les établissements. Ce nombre varie entre 1 et 36, la moitié des établissements ne définissant cependant pas plus de trois fonctions critiques (valeur médiane). La moitié centrale des réponses se situe entre deux et quatre fonctions critiques. La moyenne arithmétique est d'environ 3,5 fonctions critiques.

[1] Auto-évaluation des établissements sur une échelle de 0 à 10, où 0 = pas résilient et 10 = absolument résilient.

[2] Voir à ce sujet Cm 14 à 16 Circ.-FINMA 23/1.

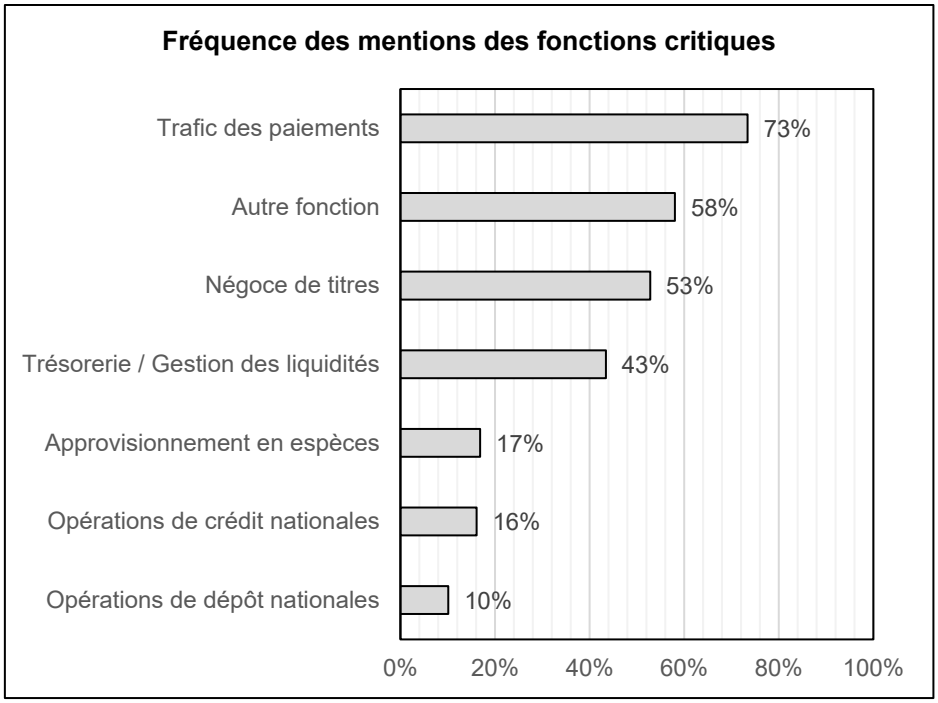


Dans la fourchette « normale », les établissements ont identifié au minimum une seule et au maximum sept fonctions critiques. Le diagramme présente en outre quelques valeurs aberrantes allant de 9 à 36 fonctions critiques.

Les données sous-jacentes permettent de conclure à l'existence d'une corrélation entre le nombre de fonctions critiques et la taille et la complexité de l'établissement : les grands établissements complexes ont défini un nombre plus élevé de fonctions critiques que les établissements de plus petite taille.

En résumé, il apparaît que la moitié centrale des établissements ont identifié entre deux et quatre fonctions critiques et que le nombre de ces dernières augmente avec la taille et la complexité de l'établissement.

Le type des fonctions critiques identifiées dépend en particulier du modèle d'affaires de l'établissement. Le graphique ci-après présente la fréquence des mentions des différents types de fonctions critiques, sachant qu'il était possible de donner plusieurs réponses.



Parmi les possibilités de réponse prédéfinies, la fonction critique la plus fréquemment identifiée par les établissements a été le trafic des paiements (73 %) et la plus rarement citée celle des opérations de dépôt nationales (10 %). Outre les possibilités de réponse prédéfinies, les établissements ont également mentionné, sous « Autre fonction », quelque 300 fonctions en texte libre. Environ deux tiers de ces fonctions (par ex. le système postal, les centrales téléphoniques, l'exploitation des systèmes informatiques, le *back-office*) sont toutefois non pas des fonctions critiques au sens des Cm 14 à 16 Circ.-FINMA 23/1, mais des processus ou des activités, ou encore des ressources sous-jacentes[3]. De plus, 71 % de toutes les fonctions critiques mentionnées dépendent directement ou indirectement de prestations de tiers.

Remarques

Avec une à sept fonctions critiques, la majorité des établissements se sont limités à un nombre peu important et donc facilement maîtrisable de fonctions, ce qui est conforme aux dispositions prudentielles[4]. Pour les établissements comptant plus de sept fonctions critiques, il y a lieu de revoir ce nombre élevé de fonctions. La question se pose notamment de savoir s'il est possible d'assurer la surveillance ainsi que la résilience opérationnelle de 25 ou même 36 fonctions critiques, comme certains établissements l'ont mentionné, et si l'exploitation d'un nombre aussi élevé de fonctions critiques a un sens du point de vue économique. De plus, en raison de la part élevée de fonctions critiques tributaires de prestations de tiers, il est particulièrement important d'avoir une vue *end-to-end* ou *front-to-back* de toute la chaîne d'approvisionnement nécessaire à leur exécution ainsi que des ressources correspondantes[5].

Le type des fonctions critiques reflète le modèle d'affaires d'un établissement et les fonctions en question doivent être clairement distinguées des processus, des activités et des ressources sous-jacentes. Les deux tiers des fonctions critiques mentionnées en texte libre doivent faire l'objet d'un examen critique à la lumière de la Circ.-FINMA 23/1. Ainsi, le *reporting* réglementaire, le respect des obligations de diligence en matière de comportement commercial *(conduct)*, la gestion et le contrôle des risques, la gestion de la clientèle, la comptabilité, les activités de *front-office* et de *back-office* ainsi que celles de représentation sont certes des composantes essentielles de l'activité des établissements. Cependant, il ne s'agit là pas de fonctions critiques au sens de la Circ.-FINMA 23/1 mais de processus qui doivent être classés comme tels. De même, le système bancaire central, l'infrastructure

[3] Voir à ce sujet les commentaires du 7 décembre 2022 « Circulaire 2008/21 ‹ Risques opérationnels – banques › – révision totale / Circulaire 2013/3 ‹ Activités d'audit › – révision partielle », ch. 4.1.8 Résilience opérationnelle (chapitre V), p. 20 à 25, disponible sous www.finma.ch > Documentation > Auditions et évaluations > Auditions achevées > 2022 > Circulaire FINMA 2008/21 « Risques opérationnels – banques » – révision totale (10.5.2022-11.7.2022) (ci-après : commentaires relatifs à la Circ.-FINMA 23/1).

[4] Voir les commentaires relatifs à la Circ.-FINMA 23/1, p. 22.

[5] Voir les commentaires relatifs à la Circ.-FINMA 23/1, p. 22.

informatique et son exploitation ainsi que la téléphonie, par exemple, ne sont pas des fonctions critiques d'ordre stratégique, mais doivent être qualifiés de ressources sous-jacentes. Enfin, diverses autres fonctions mentionnées, telles que la connectivité, la disponibilité des systèmes et la joignabilité des personnes sont simplement des indicateurs de surveillance de l'inventaire des fonctions critiques.

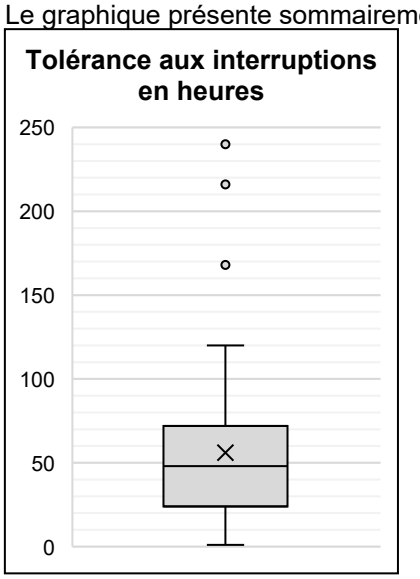
Les processus et les ressources sous-jacentes servent l'objectif d'ordre supérieur consistant à assurer l'exécution des fonctions critiques. En effet, la défaillance d'une telle fonction a toujours un impact direct et immédiat sur la clientèle de l'établissement, sur l'établissement lui-même ou sur le bon fonctionnement du marché financier dans son ensemble. Ainsi, lors de l'identification des fonctions critiques, il convient d'adopter un point de vue stratégique et de suivre une approche descendante, de manière à ne définir comme étant des fonctions critiques que les opérations ou les prestations les plus importantes sur le plan stratégique.

Dans l'inventaire des fonctions critiques, il y a lieu de présenter, outre les fonctions critiques elles-mêmes, notamment les processus et les ressources sous-jacents ainsi que leurs interdépendances. Une présentation sous la seule forme d'un tableau sans indication des dépendances internes n'a pas valeur d'inventaire des fonctions critiques au sens du Cm 107 Circ.-FINMA 23/1.

3.2 Tolérances aux interruptions

Enseignements

Le graphique présente sommairement les tolérances aux interruptions, exprimées en heures, de toutes les fonctions critiques définies par les établissements interrogés. Il montre que la majorité des établissements ont choisi de mesurer la tolérance aux interruptions au moyen d'une unité de temps. Seuls quelques-uns ont défini comme paramètre de tolérance, en lieu et place du temps, le taux d'annulation ou le taux d'erreur, ou encore une valeur limite inférieure, par exemple pour les liquidités.



Les tolérances aux interruptions varient entre 1 et 8 736 heures (365 jours)[6], la moitié des établissements définissant

[6] Conformément à la Circ.-FINMA 23/1, les fonctions présentant une tolérance aux interruptions supérieure à 10 jours / 240 heures doivent être réexaminées quant à leur caractère critique. Afin de

une tolérance ne dépassant pas 48 heures (valeur médiane). La moitié centrale des tolérances définies se situe entre 24 et 72 heures. La moyenne arithmétique est de 56 heures.

Les données sous-jacentes ne permettent pas de conclure à l'existence d'une corrélation entre les tolérances aux interruptions et la taille et la complexité des établissements. La tolérance aux interruptions est définie – comme les dispositions prudentielles le prévoient – en fonction du type de fonction critique ainsi que des répercussions sur celle-ci.

En résumé, il apparaît que la moitié centrale des établissements ont défini des tolérances aux interruptions se situant entre 24 et 72 heures, indépendamment de la taille et de la complexité de l'établissement.

Par ailleurs, dans le cadre de ses activités de surveillance ainsi qu'à la faveur des « Horizontal Reviews Operational Resilience 2025 »[7], la FINMA a constaté, en ce qui concerne les établissements des catégories de surveillance 1 à 3, que les tolérances aux interruptions ont été en partie définies sur la base de la capacité de rétablissement de l'établissement prévue dans un scénario grave mais plausible (rétro-ingénierie) et non sur la base de la tolérance de l'organe responsable de la haute direction.

Remarques

La définition des tolérances aux interruptions peut reposer, outre sur la dimension temporelle, sur d'autres critères de mesure, tels que le préjudice financier ou la perte de clientèle. Le cas échéant, les répercussions auxquelles il faut s'attendre sur les relations clientèle, sur l'établissement lui-même et sur le bon fonctionnement du marché financier dans son ensemble revêtent une importance capitale.

Les exigences prudentielles prévoient que les tolérances aux interruptions doivent refléter la tolérance de l'organe responsable de la haute direction face aux chocs, indépendamment de la capacité de rétablissement de l'établissement[8]. Le recours à la rétro-ingénierie n'est donc pas conforme aux dispositions prudentielles.

Les valeurs aberrantes de moins de 24 heures de tolérance aux interruptions doivent être revues. Il y a lieu, d'une part, d'examiner si les fonctions critiques concernées sont effectivement des fonctions critiques au sens de la Circ.-FINMA 23/1 (voir ch. 3.1) ou s'il ne s'agit pas simplement de processus critiques, dont les valeurs de tolérance sont définies sous la forme de

simplifier l'analyse et d'en améliorer la lisibilité, toutes les valeurs dépassant 10 jours / 240 heures ont été exclues du diagramme en boîte et n'ont pas non plus été prises en compte dans les calculs des valeurs moyennes.

[7] Au moment de la publication de la présente communication sur la surveillance, les évaluations « Horizontal Reviews Operational Resilience 2025 » n'étaient pas toutes achevées.

[8] Voir Cm 101 Circ.-FINMA 23/1.

RTO/RPO[9] dans le *business continuity management* (BCM). D'autre part, il faut également examiner si la définition et le calibrage de la tolérance aux interruptions sont adéquats et si les dimensions « relations clientèle », « poursuite de l'établissement » et « bon fonctionnement du marché financier » ont été prises en considération de manière appropriée.

Pour les tolérances aux interruptions définies à un niveau très bas, il y a lieu d'examiner de manière critique en particulier leur dépendance à l'égard de prestataires et de fournisseurs externes et d'en assurer une communication transparente tout au long de la chaîne d'approvisionnement. Ainsi, il faut définir la tolérance aux interruptions conformément à une vue *end-to-end* ou *front-to-back* de toute la chaîne d'approvisionnement et prendre en considération les ressources nécessaires à cet effet[10].

Les tolérances aux interruptions dépassant 240 heures (dix jours) sont quant à elles très élevées. Une fonction à laquelle la clientèle, l'établissement et le marché financier peuvent renoncer pendant plus de dix jours – et cela en l'absence de rétablissement partiel de la fonction, de système de substitution *(fallback)*, de solution de contournement *(workaround)* ou autre – n'est probablement pas critique pour l'établissement. La FINMA recommande donc que ces tolérances aux interruptions particulièrement élevées soient réexaminées la prochaine fois qu'elles seront soumises à l'approbation de l'organe responsable de la haute direction.

Les tolérances aux interruptions dépassant 120 heures (cinq jours) doivent aussi être revues. La question se pose en effet de savoir si les relations clientèle et l'établissement lui-même peuvent surmonter une tolérance aussi élevée. Lors de la définition des tolérances aux interruptions, il est également possible de définir une tolérance inférieure à la capacité de rétablissement actuelle de l'établissement. Dans ce cas (hors tolérance), il y a lieu de prendre des mesures propres à garantir la résilience opérationnelle, afin d'entrer dans la fourchette de tolérance.

3.3 Tests

Enseignements

Les tests servent à identifier les points faibles de la résilience opérationnelle et permettent ainsi de l'améliorer. La FINMA a constaté que, au moment de l'enquête, 85 % des établissements des catégories de surveillance 1 à 3 n'avaient pas encore effectué de tests.

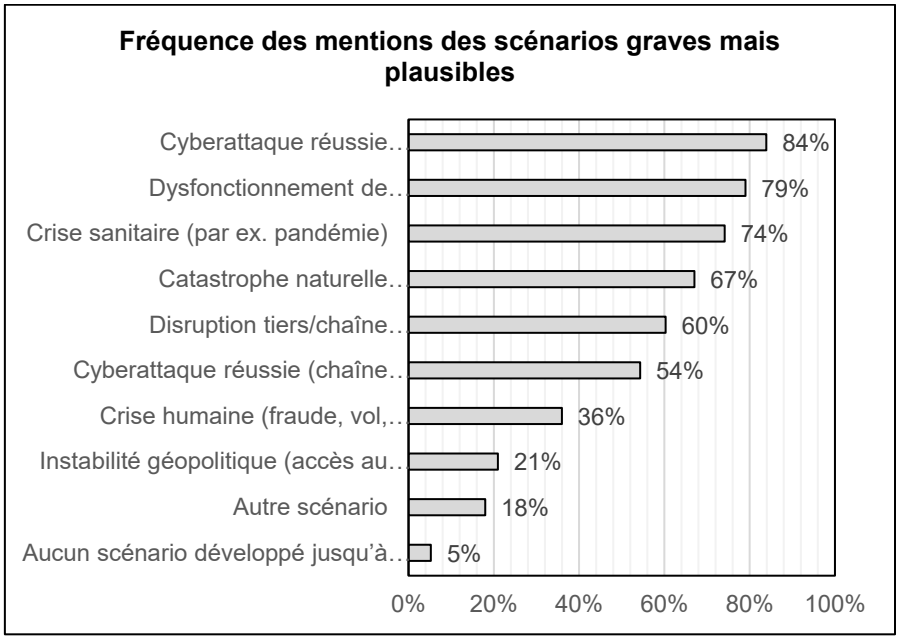
Une part de 10 % des établissements avaient déjà planifié la réalisation de tests, dont une nette majorité (72 %) prévoient d'en effectuer annuellement.

[9] RTO : *recovery time objective* ; RPO : *recovery point objective* ; voir Cm 10 Circ.-FINMA 23/1.

[10] Voir les commentaires relatifs à la Circ.-FINMA 23/1, p. 22.

Les quelque 5 % restants des établissements n'avaient encore ni effectué ni planifié de tests.

Le graphique ci-après présente les scénarios graves mais plausibles que les établissements ont mentionnés parmi les possibilités de réponses prédéfinies en matière de tests.



Dans l'enquête, 84 % des établissements ont mentionné une « Cyberattaque réussie (établissement) » comme scénario grave mais plausible à intégrer dans leurs procédures de test. Le scénario « Cyberattaque réussie (chaîne d'approvisionnement) » a été mentionné par 54 % des établissements et celui de « Disruption tiers/chaîne d'approvisionnement (externalisation) » par 60 %. Parmi les établissements interrogés, 18 % ont défini d'autres scénarios et 5 % n'en avaient encore élaboré aucun.

Remarques

Les établissements des catégories de surveillance 1 à 3 sont tenus d'effectuer des tests à intervalles réguliers[11]. Il s'agit en l'occurrence d'en tester la capacité à exécuter des fonctions critiques dans les limites de leurs tolérances aux interruptions en cas de scénarios graves mais plausibles.

Lors de la planification et de la conception des tests, il faut s'appuyer en particulier sur une vue *end-to-end* ou *front-to-back* de toute la chaîne d'approvisionnement et des ressources nécessaires à l'exécution de la fonction critique[12]. À cet égard, la réalisation de tests transversaux à l'échelle de l'établissement peut présenter des avantages, de même que la réalisation de

[11] Voir Cm 20 et 110 Circ.-FINMA 23/1.

[12] Voir les commentaires relatifs à la Circ.-FINMA 23/1, p. 22.

tests en association avec d'autres établissements. De plus, la totalité des éléments à tester doivent pouvoir être examinés par l'organe responsable de la haute direction, afin de permettre une évaluation indépendante du dispositif de résilience opérationnelle[13].

La FINMA rappelle que les établissements assujettis sont tenus d'élaborer des scénarios graves mais plausibles et d'en tester le déroulement, le tout sur la base des menaces potentielles spécifiques à l'établissement[14]. Il convient de continuer à développer en particulier l'analyse des menaces et des vulnérabilités liées aux activités « non cyber », qui n'a pas encore atteint le degré de maturité requis dans certains établissements.

3.4 Dispositif de résilience opérationnelle

Enseignements

Au vu des résultats de l'enquête, la FINMA a constaté que seuls 12 à 15 %[15] des établissements des catégories de surveillance 1 à 3 interrogés coordonnaient déjà les principales composantes existantes[16] de leur activité pour renforcer leur résilience opérationnelle. Cette intégration était donc encore loin d'être complète sur le marché.

Environ 60 % des établissements interrogés utilisent leurs propres chiffres clés et indicateurs[17] aux fins de la surveillance de leur résilience opérationnelle et du dispositif mis en œuvre pour la garantir. Le nombre d'indicateurs ou chiffres clés définis par établissement pour surveiller et gérer la résilience opérationnelle varie entre un seul et 31.

Remarques

À partir du 1er janvier 2026, les établissements des catégories de surveillance 1 à 3 auront l'obligation de coordonner leur dispositif visant à garantir leur résilience opérationnelle avec les autres composantes importantes de leur activité, telles que la gestion des risques opérationnels – y compris la

[13] Voir Cm 103 Circ.-FINMA 23/1.

[14] Voir Cm 70 Circ.-FINMA 23/1, en relation avec la communication FINMA sur la surveillance 03/2024.

[15] En fonction de la composante prudentielle concernée.

[16] Gestion des risques opérationnels – y compris la gestion des risques TIC et des cyberrisques –, *business continuity management* (BCM), gestion des parties tierces et plan d'urgence.

[17] Par exemple pour le monitorage de la fin de vie, la disponibilité du système bancaire central et la stabilité des systèmes informatiques : durée cumulée des perturbations / défaillances inattendues, nombre de vulnérabilités critiques, part des retards de gestion des points faibles, nombre d'incidents relevant du centre des opérations de sécurité (*security operation center*, SOC), nombre de cybercontrôles clés non réussis, nombre d'événements relevant de la prévention des pertes de données (*data loss prevention*, DLP), nombre de cas de dépassement des valeurs RTO/RPO, nombre d'incidents majeurs non encore résolus, nombre d'irrégularités / de mesures ressortant d'audits non encore prises en compte, nombre de *business continuity plan* (BCP) activés, nombre de violations de *service level agreements* (SLA) réglant des externalisations essentielles, nombre de défaillances de personnes clés.

gestion des risques TIC et des cyberrisques –, le *business continuity management* (BCM), la gestion des parties tierces et le plan d'urgence, afin de renforcer leur résilience opérationnelle à long terme[18].

Cela nécessite de procéder à des échanges appropriés d'informations pertinentes entre les composantes concernées. Ces échanges d'informations ainsi que la définition de chiffres clés pertinents sont les conditions essentielles de l'efficacité des mesures mises en œuvre pour garantir la résilience opérationnelle[19]. Ils permettent, d'une part, de contrôler l'efficacité du dispositif mis en place et, d'autre part, d'évaluer la résilience opérationnelle de l'établissement à l'aide d'indicateurs indépendants.

4 Conclusion et prochaines étapes

Dans le cadre de son activité de surveillance et conformément à l'exigence prudentielle d'une gestion des risques appropriée, la FINMA accorde une grande importance à la résilience opérationnelle des établissements. Elle se concentre en particulier sur la résilience des fonctions critiques, indépendamment de la taille et de la complexité de l'établissement.

Les enseignements tirés de l'enquête ainsi que des entretiens de surveillance régulièrement menés par la FINMA et des « Horizontal Reviews Operational Resilience 2025 »[20] permettent de brosser un tableau qui présente encore une très grande hétérogénéité en ce qui concerne l'interprétation des exigences prudentielles ainsi que la mise en œuvre et le degré de maturité de la résilience opérationnelle dans les établissements assujettis.

À partir du 1er janvier 2026, les établissements auront l'obligation, quelle que soit leur catégorie de surveillance, de prendre des mesures visant à garantir leur résilience opérationnelle, compte tenu de scénarios graves mais plausibles[21]. En améliorant ainsi la résilience opérationnelle de chaque établissement, ces mesures devraient contribuer à renforcer la résilience opérationnelle de l'ensemble du marché financier suisse.

Les établissements devront donc continuer à se concentrer sur les activités visant à garantir leur résilience opérationnelle de manière préventive ainsi que sur les mesures leur permettant de développer leur modèle opérationnel à la faveur d'un processus d'amélioration continue, de manière à assurer la résilience de leurs fonctions critiques *(resilience by design)*.

[18] Voir Cm 104 et 113 Circ.-FINMA 23/1.

[19] Voir Cm 102 et 113 Circ.-FINMA 23/1.

[20] Au moment de la publication de la présente communication sur la surveillance, les évaluations « Horizontal Reviews Operational Resilience 2025 » n'étaient pas toutes achevées.

[21] Voir Cm 102 et 113 Circ.-FINMA 23/1.

Dans le même temps, la FINMA poursuivra et intensifiera ses activités de surveillance spécifiques aux établissements destinées à en garantir la résilience opérationnelle. Elle prévoit en particulier d'approfondir les analyses de scénarios et de créer à long terme les conditions nécessaires à la réalisation de tests à l'échelle du secteur. Enfin, la FINMA observe également les développements internationaux, notamment au sein de l'AICA[22], et examine s'il serait opportun d'étendre les exigences prudentielles visant à garantir la résilience opérationnelle à d'autres établissements soumis à sa surveillance.

[22] AICA : Association internationale des contrôleurs d'assurance