CENTRE DE DROIT
BANCAIRE ET FINANCIER

Surveillance FINMA

Une nouvelle circulaire pour les risques opérationnels

Par Célian Hirsch le 19 décembre 2022

De nouvelles normes internationales et de fortes évolutions dans le domaine de la numérisation. Voici les deux facteurs invoqués par la FINMA pour justifier la révision de sa Circulaire 08/21 sur les risques opérationnels. Adoptée le 7 décembre 2022, la Circulaire 2023/1 entrera en vigueur le 1er janvier 2024.

La nouvelle circulaire distingue la gestion globale des risques opérationnels et la gestion de risques opérationnels spécifiques. Ces derniers sont notamment ceux liés aux technologies de l'information et de la communication (TIC), aux cyberrisques, aux données critiques, et, enfin, aux activités de service transfrontières. Le présent commentaire se concentre sur les trois premiers types de risques, avant d'aborder brièvement une nouveauté de la circulaire : la résilience opérationnelle.

Les risques opérationnels correspondent aux risques « de pertes financières résultant de l'inadéquation ou de la défaillance de processus ou de systèmes internes, d'actions inappropriées de personnes ou d'erreurs qu'elles ont commises ou encore d'événements externes ». La définition correspond à celle de l'art. 89 de l'Ordonnance sur les fonds propres et celle du Comité de Bâle sur le contrôle bancaire (CBCB). L'élément central est celui de pertes financières, qui est compris de manière large. Cela inclut par exemple les cyberattaques qui résultent en une perte de confiance des clients, même si la perte financière n'est pas directement quantifiable.

L'évolution numérique impose aux assujettis une bonne gestion des changements liés à la TIC (*change management*), son exploitation (*run*, *maintenance*) et la gestion des incidents. Concernant le premier aspect, l'assujetti doit en particulier garantir la séparation entre, d'une part, les environnements de développement ou de test et, d'autre part, l'environnement de production TIC. Concernant le deuxième, l'assujetti doit disposer d'un inventaire qui comprend les composantes matérielles et logicielles ainsi que les lieux de sauvegarde des données critiques. Enfin, en cas d'incident TIC important, l'assujetti doit notamment en informer la FINMA sans délai.

La gestion des cyberrisques impose également un devoir d'informer la FINMA des cyberattaques, mais ce devoir n'est pas nouveau (et il sera probablement revu prochainement afin de s'adapter à une future obligation plus générale d'annonce des cyberattaques). L'obligation principale réside dans la mise en place d'une stratégie contre les cyberattaques. Cette stratégie doit comprendre des processus et des contrôles afin (a) d'identifier des

menaces spécifiques et potentielles liées aux cyberattaques, (b) de protéger la confidentialité, l'intégrité et la disponibilité des données électroniques critiques et des composantes TIC, (c) de détecter rapidement des cyberattaques et, enfin, (d) de réagir aux vulnérabilités et (e) de rétablir rapidement la marche des affaires après une cyberattaque. Par ailleurs, l'assujetti doit procéder à des tests d'intrusion et des cyberexercices.

Dans l'annexe 3 de la Circulaire 08/21, la FINMA imposait une protection particulière des « données d'identification du client » (CID). L'accent était alors mis sur la confidentialité de ces seules données. Conformément aux développements technologiques, la protection s'applique désormais à toutes les données importantes sous l'angle tant de la confidentialité que de l'intégrité et de la disponibilité (mais non sous l'aspect de leur traçabilité).

La Circulaire 23/1 impose ainsi une protection particulière aux données dites « critiques » (« *critical information assets* » selon la terminologie du CBCB). Alors que le projet de circulaire prévoyait une définition large des « données critiques », c'est une définition proche de celle proposée par l'Association suisse des banquiers qui a été retenue. Les données critiques sont les « données qui, compte tenu de la taille, de la complexité, de la structure, du profil de risque ainsi que du modèle d'affaires de l'établissement revêtent une importance telle qu'elles nécessitent des exigences accrues en matière de sécurité ». Il appartient à chaque assujetti d'identifier ses données critiques.

Une fois identifiées, ces données sont soumises à des mesures de protection particulières. Ces mesures comprennent non seulement un accès limité par les employés (principe du *need to know*) ainsi qu'une formation et surveillance de ceux-ci, mais aussi une protection et une surveillance des données lorsqu'elles sont conservées hors de Suisse ainsi qu'une *due diligence* des prestataires qui traitent ces données. Enfin, tout incident important lié aux données critiques doit être annoncé immédiatement à la FINMA.

La Circulaire 23/1 contient finalement des exigences en matière de résilience opérationnelle. L'intégration de ces exigences est justifiée par l'augmentation de « chocs opérationnels », tels que des pandémies, des cyberattaques, des défaillances systémiques, des pannes dans les chaînes d'approvisionnement, des coupures d'électricité étendues ou durables, ou encore des catastrophes naturelles.

La résilience opérationnelle a aussi fait l'objet de nouvelles règlementations au niveau international. Le CBCB a adopté en mars 2021 ses *Principles for operational resilience*. Plus récemment, en novembre 2022, le Conseil de l'Union européenne a approuvé le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA, cf. cdbf.ch/1164/). Son entrée en vigueur se fera de manière progressive sur deux ans, comme les règles relatives à la résilience dans la Circulaire 23/1. Cependant, et à la différence du droit suisse, le règlement DORA s'applique non seulement aux entités financières, mais également aux prestataires tiers de services TIC, tels que les prestataires *cloud*.

---

financier, https://cdbf.ch/1265/