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 04/2024

Gestion des risques opérationnels des directions de fonds et des gestionnaires de fortune collective

12 juin 2024

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

Table des matières

1 Introduction

Pour assurer une protection efficace des investisseurs, les directions de fonds et les gestionnaires de fortune collective (ci-après les établissements) doivent disposer d'une gestion des risques qui fonctionne bien.

La gestion des risques couvre l'ensemble des risques principaux auxquels les établissements, au travers de leurs activités et des fortunes collectives qu'ils gèrent et d'autres fortunes gérées, sont ou pourraient être exposées (voir art. 9 et 26 de la loi sur les établissements financiers [LEFin ; RS *954.1*], art. 12 al. 4, art. 41 et art. 57 de l'ordonnance sur les établissements financiers [OEFin ; RS *954.11*] ainsi qu'art. 8 ss et art. 18 de l'ordonnance de la FINMA sur les établissements financiers [OEFin-FINMA ; RS *954.111*]).

Les risques opérationnels font partie de ces risques principaux. Comme pour les autres établissements assujettis à la surveillance de la FINMA, les risques opérationnels auxquels sont exposés les directions de fonds et les gestionnaires de fortune collective augmentent, comme le révèlent notamment les annonces relatives aux cyberattaques. Parallèlement, la FINMA constate, dans le cadre des procédures d'autorisation et de l'activité de surveillance, un nombre croissant de lacunes et de points faibles dans la gestion des risques opérationnels des directions de fonds et des gestionnaires de fortune collective.

La présente communication sur la surveillance s'adresse donc à ces établissements pour leur rappeler l'importance d'une gestion adéquate des risques opérationnels et de leur indiquer des mesures possibles.

Dans la présente communication sur la surveillance, comme dans la circulaire FINMA 2023/1 « Risques et résilience opérationnels – banques »[1], on entend par risque opérationnel le risque 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. Sont aussi comprises les pertes financières qui peuvent découler des risques juridiques ou de *compliance*. À cet égard, la gestion des risques opérationnels doit également prendre en compte d'autres types de dommages[2], dès lors que ceux-ci peuvent aussi se traduire par des pertes financières. Les risques stratégiques sont toutefois exclus.

[1] www.finma.ch > Documentation > Circulaires

[2] Par exemple répercussions négatives sur la réputation, perte potentielle de confiance et perte de clientèle, incidences négatives sur le marché, conséquences réglementaires négatives (par ex. perte potentielle de licence).

2 Exemples de lacunes et de points faibles constatés

Des exemples de lacunes et de points faibles récemment constatés en matière de gestion des risques opérationnels sont présentés ci-après.

2.1 Processus et procédures en général

Des erreurs dans la saisie de transactions ou les décomptes de transactions n'ont été constatées qu'après la survenance d'un dommage, du fait de l'absence de contrôles ou de contrôles effectués trop tard.

2.2 Technologies de l'information et de la communication et sécurité des données

Lors de l'introduction de solutions *cloud* pour le stockage de données des clients et de l'entreprise, la sélection et surtout le contrôle des prestataires de services *cloud*, la question des droits d'accès, la sécurité des données et l'intégration dans la gestion de la continuité des affaires *(business continuity management)* ou dans les plans de continuité des affaires n'ont pas, ou pas suffisamment, été pris en compte.

L'identification d'une infrastructure comme étant essentielle, notamment les technologies de l'information et de la communication, nécessaire à l'exercice des activités essentielles de l'établissement, n'a pas été effectuée ou l'a été de manière insuffisante. De ce fait, cette infrastructure n'était pas protégée de manière adéquate et n'était pas prise en compte de manière adéquate dans les plans de continuité des affaires.

2.3 Cyberrisques

Des attaques d'hameçonnage réussies ont permis à des tiers non autorisés d'accéder à des données critiques d'établissements, y compris à des données d'accès à des applications essentielles. Au moyen de ces données dérobées, il a notamment été tenté d'effectuer des transactions non autorisées.

Des établissements qui ont externalisé leur comptabilité auprès d'un prestataire externe ont temporairement perdu la vue d'ensemble et le contrôle de leur situation financière, et donc en particulier la capacité de surveiller leur situation en matière de fonds propres, à la suite de cyberattaques réussies contre le prestataire en question.

Les établissements ont certes été en mesure de détecter rapidement les cyberattaques, mais ils ne disposaient d'aucun plan sur la manière de réagir à de telles attaques ni sur la manière dont étaient réglées les compétences dans de tels cas.

Enfin, les établissements n'avaient pas conscience du fait qu'ils sont tenus d'annoncer les cyberattaques à la FINMA conformément à la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA »[3]. Ils ne savaient pas non plus qu'une annonce doit être faite au Préposé fédéral à la protection des données et à la transparence (PFPDT)[4].

2.4 Gestion de la continuité des affaires (*business continuity management)*

Les plans élaborés dans le cadre de la gestion de la continuité des affaires (plans de continuité des affaires) ne couvraient pas l'ensemble des ressources essentielles nécessaires à la réalisation des activités essentielles actuelles, notamment en termes de ressources humaines et techniques. Les établissements ne pouvaient donc pas garantir le maintien de leurs activités essentielles ou la reprise rapide de celles-ci en cas de crise.

Les plans de continuité des affaires n'ont pas été testés ou ne l'ont pas été régulièrement, ce qui a entraîné ou pourrait entraîner des retards importants dans la réparation des dommages survenus.

2.5 Risques juridiques et de *compliance*

Dans le cadre de la gestion de fortune individuelle, des établissements ont employé des instruments financiers ou appliqué des techniques de placement inappropriés pour les clients concernés ou qui ne correspondaient pas à ce qui était convenu.

Des établissements qui fournissent notamment des services de gestion de fortune individuelle n'ont pas suffisamment tenu compte du domicile des clients cibles dans le cadre des analyses de risque prescrites par la législation sur le blanchiment d'argent.

Des établissements disposaient certes de directives internes en matière d'activités transfrontières et de guides relatifs aux pays correspondants mais les contrôles et compétences prévus dans ces documents n'étaient pas, ou insuffisamment, observés.

[3] www.finma.ch > Documentation > Communications FINMA sur la surveillance

[4] Voir l' obligation d'annoncer au Préposé fédéral à la protection des données et à la transparence (PFPDT) les cas de violation de la sécurité des données conformément à l'art. 24 de la loi sur la protection des données (LPD), voir le service en ligne d'annonce de violation de la sécurité des données (art. 24 LPD).

2.6 Externalisations d'activités essentielles

Lors du choix des prestataires auprès desquels la gestion des risques opérationnels devait être externalisée, trop peu d'importance a été accordée aux connaissances et à l'expérience des prestataires en question dans le domaine de la gestion des risques opérationnels (voir Cm 16 à 21 de la circulaire FINMA 2018/3 « *Outsourcing* »[5] sur les exigences régissant le choix, l'instruction et le contrôle du prestataire).

Les activités externalisées n'ont pas été saisies ou l'ont été de manière incorrecte (voir Cm 14 à 15.1 Circ.-FINMA 18/3 sur l'inventaire des fonctions externalisées). Cela s'est traduit par des lacunes dans les contrôles ou par une prise en compte insuffisante de ces activités externalisées dans la gestion des risques opérationnels.

3 Exigences générales en matière de gestion des risques

3.1 Gestion des risques en général

Pour éviter des points faibles et lacunes similaires à ceux évoqués ci-avant, la FINMA rappelle aux directions de fonds et aux gestionnaires de fortune collective les exigences générales en matière de gestion appropriée des risques.

L'organe responsable de la haute direction, de la surveillance et du contrôle fixe dans des directives internes les principes de gestion de tous les risques principaux auxquels l'établissement, par le biais de son activité, et de la fortune qu'il gère, est exposé. Il doit aussi déterminer la tolérance au risque.

Sur la base des directives de l'organe responsable de la haute direction, de la surveillance et du contrôle, l'organe responsable de la gestion doit élaborer des instructions, des procédures et des processus appropriés pour identifier, évaluer, maîtriser et contrôler les risques. Il doit en outre désigner les fonctions ou les personnes compétentes et responsables en la matière et garantir qu'un compte rendu périodique pertinent est établi à l'intention de l'organe responsable de la haute direction, de la surveillance et du contrôle.

L'organe responsable de la haute direction, de la surveillance et du contrôle ainsi que l'organe responsable de la gestion doivent vérifier régulièrement l'adéquation et l'efficacité des principes, de la tolérance au risque, des instructions, des procédures et des processus de la gestion des risques, en particulier en cas de changement d'activité ou d'organisation.

[5] www.finma.ch > Documentation > Circulaires

3.2 Gestion des risques opérationnels dans le cadre de la gestion des risques

Les risques opérationnels font partie des risques principaux auxquels sont exposés les directions de fonds et les gestionnaires de fortune collective ainsi que les fortunes qu'ils gèrent. Les exigences susmentionnées s'appliquent par conséquent aussi à la gestion des risques opérationnels. Cela signifie en particulier que les personnes chargées de la gestion des risques opérationnels doivent disposer des connaissances et de l'expérience requises.

4 Gestion des risques opérationnels

4.1 Principes généraux de la gestion des risques opérationnels et de son organisation

La condition préalable à une gestion efficace des risques opérationnels à l'échelle de l'établissement est la prise en compte de l'activité et de l'organisation effectives de l'établissement. À cet égard, il convient en particulier de tenir compte des procédures et processus appliqués pour la réalisation de cette activité ainsi que des ressources humaines et techniques employées et des données nécessaires.

Lors de la conception des processus et procédures opérationnels, l'établissement doit prévoir des mesures et des contrôles adéquats (par ex. principe du double contrôle) pour en garantir l'efficacité et la fiabilité.

4.2 Éléments spécifiques de la gestion des risques opérationnels

4.2.1 Risques liés aux technologies de l'information et de la communication

Un inventaire des principales composantes matérielles et logicielles utilisées par l'établissement dans le cadre des processus et procédures pour réaliser ses activités essentielles constitue la base d'une gestion efficace des risques liés aux technologies de l'information et de la communication.

L'établissement détermine la tolérance au risque pour ces principales composantes matérielles et logicielles et prend les mesures nécessaires pour en garantir la disponibilité, la confidentialité et l'intégrité telles que définies.

4.2.2 Risques liés aux données critiques

Les données qui sont particulièrement dignes de protection (par ex. les données des clients) ou critiques pour l'activité de l'établissement doivent être identifiées et des mesures de protection adéquates doivent être prises pour en préserver la disponibilité, la confidentialité et l'intégrité.

Cela implique aussi de définir clairement les tâches, les compétences et les responsabilités ainsi que les contrôles relatifs au traitement des données critiques.

4.2.3 Cyberrisques

Sur la base de leur activité et de leur organisation, les établissements doivent analyser et identifier les menaces potentielles liées aux cyberattaques, prendre des mesures de protection adéquates en conséquence et assurer la surveillance de leur infrastructure d'information et de communication.

Il est attendu que les collaborateurs soient régulièrement formés et sensibilisés au traitement des cyberrisques.

L'établissement doit prévoir des mesures permettant une reprise rapide de la marche ordinaire des affaires après une cyberattaque réussie ou partiellement réussie. Il doit en outre s'assurer qu'il remplit correctement son obligation d'annoncer les cyberattaques[6].

Dans le contexte du traitement des cyberrisques en particulier, il est important que l'établissement ait clairement défini les tâches, les compétences et les responsabilités, en tenant compte de la communication éventuelle, en particulier avec les clients, les partenaires commerciaux et, le cas échéant, d'autres personnes concernées.

4.2.4 Gestion de la continuité des affaires

Les établissements doivent élaborer en fonction de leurs activités et de leur organisation un plan de continuité des affaires pour, en cas de crise, le maintien et le rétablissement des processus et procédures essentiels à ses activités.

Il est important de vérifier périodiquement le plan de continuité des affaires et de l'actualiser si nécessaire. Il y a en outre toujours lieu de vérifier, et le

[6] Voir l'obligation d'annoncer les cyberattaques selon l'art. 29 al. 2 LFINMA et communication FINMA sur la surveillance 05/2020 (voir note de bas de page 3) ainsi que l'obligation d'annoncer au Préposé fédéral à la protection des données et à la transparence (PFPDT) les cas de violation de la sécurité des données conformément à l'art. 24 de la loi sur la protection des données (LPD ; RS **235.1**) (voir note de bas de page 4).

cas échéant adapter, le plan de continuité des affaires lorsque des modifications sont apportées aux activités et à l'organisation.

Les plans de continuité des affaires doivent être testés périodiquement, en particulier lorsque les établissements ont des activités importantes ou complexes.

Enfin, il est important que les établissements disposent d'une stratégie de communication claire en cas d'urgence et qu'ils aient déterminé clairement les tâches et les compétences.

4.2.5 Gestion des risques juridiques et de *compliance*, en particulier ceux liés aux activités transfrontières

Les établissements qui fournissent des prestations ou distribuent des instruments financiers dans le cadre d'activités transfrontières doivent s'assurer qu'ils identifient, limitent et contrôlent de manière adéquate les risques qui en découlent.

Les établissements doivent procéder à une analyse des conditions-cadres juridiques de l'activité de prestations transfrontière ainsi que de la distribution transfrontière d'instruments financiers ainsi que des risques qui en découlent et prendre les mesures nécessaires de réduction des risques.

La situation juridique pertinente dans les pays concernés doit être observée en permanence et les mesures de réduction des risques adaptées si nécessaire.

4.2.6 Gestion des risques opérationnels en cas d'externalisations

4.2.6.1 Externalisation de la gestion des risques et de la *compliance*

Même en cas d'une éventuelle externalisation de la gestion des risques et de la *compliance* à des tiers, il incombe aux établissements de s'assurer que les mesures de gestion des risques opérationnels sont prises. Lors du choix des tiers auprès desquels la gestion des risques doit être externalisée, les établissements doivent donc aussi accorder de l'importance aux connaissances et à l'expérience des tiers en question dans le domaine de la gestion des risques opérationnels.

4.2.6.2 Externalisation d'activités essentielles

Les établissements qui externalisent d'autres activités essentielles pour leur activité à des tiers ou qui ont recours à des tiers pour des ressources nécessaires au procédures et systèmes essentiels doivent remplir les exigences

de la Circ.-FINMA 18/3[7] (notamment en ce qui concerne l'inventaire des fonctions externalisées ainsi que le choix, l'instruction et le contrôle du prestataire). Les établissements doivent aussi veiller à ce que les fonctions externalisées soient intégrées dans la gestion des risques opérationnels.

[7] Voir note de bas de page 5.