Février 2026

Synthèse des contrôles SPOT relative au dispositif de gestion des risques opérationnels des sociétés de gestion de portefeuille

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

Table des matières

1- CONTEXTE

Comme annoncé à l'occasion de ses priorités[1] de supervision pour l'année 2025, l'Autorité des marchés financiers (« **AMF** ») a diligenté une campagne de contrôles SPOT (Supervision des Pratiques Opérationnelle et Thématique) sur le dispositif de gestion des risques opérationnels déployé au sein des sociétés de gestion de portefeuille (« **SGP** »).

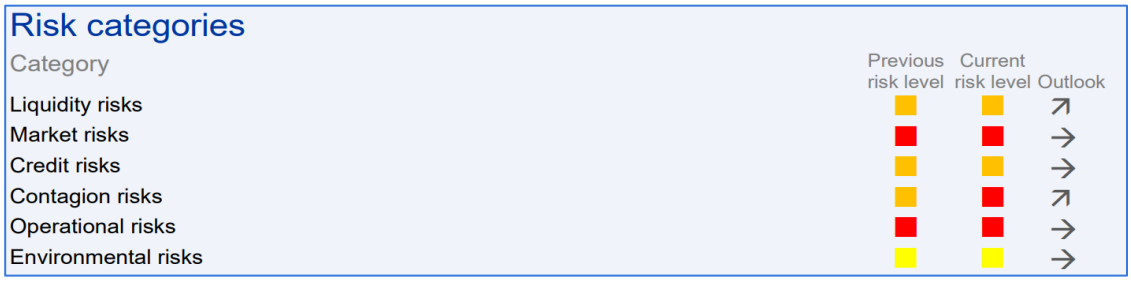
Le **risque opérationnel** est défini par la réglementation[2] comme le risque de perte, pour un portefeuille géré, résultant de l'inadéquation de processus internes et de défaillances liées aux personnes et aux systèmes de la SGP, ou résultant d'événements extérieurs, y compris le risque juridique et le risque de documentation, ainsi que le risque résultant des procédures de négociation, de règlement et d'évaluation, appliquées pour le compte du portefeuille géré.

Les SGP doivent mettre en place des politiques et des procédures de gestion des risques leur permettant d'évaluer, de façon périodique, l'exposition de chaque portefeuille géré au risque opérationnel susceptible d'être significatif. Elles doivent plus généralement **identifier, mesurer, gérer et surveiller** les risques opérationnels, en établissant notamment des limites de risque et en veillant à les respecter.

De plus, lorsqu'elles confient à un tiers l'exécution de tâches ou de fonctions opérationnelles essentielles ou importantes pour la fourniture d'un service ou l'exercice d'activités, les SGP doivent prendre des mesures raisonnables pour éviter une aggravation indue du risque opérationnel.

Les SGP soumises à la directive 2011/61/UE du 8 juin 2011 (dites « **directive AIFM**[3] ») doivent, par ailleurs, choisir de couvrir leurs risques en matière de responsabilité professionnelle, soit par des fonds propres supplémentaires appropriés, soit par une assurance de responsabilité civile professionnelle (« **RCP** ») adaptée aux risques couverts.

Dans son *Trends, Risks and Vulnerabilities Report n°2 (2025)*[4], l'ESMA[5] place le risque opérationnel au niveau le plus élevé[6] de ses préoccupations, au même titre que le risque de marché, confirmant se faisant la tendance observée en 2024.



Un dispositif robuste de gestion des risques opérationnels est donc indispensable au respect des obligations professionnelles des SGP, quelle que soit leur taille. En contribuant à fiabiliser les processus internes et à améliorer les capacités de continuité des activités, un tel dispositif œuvre à la protection des investisseurs.

---

1 https://www.amf-france.org/fr/actualites-publications/publications/rapports-annuels-et-documents-institutionnels/priorites-de-supervision-de-lamf-pour-2025

2 Cf. « cadre règlementaire » dans la section 2 *infra*.

3 *Alternative investment fund management.*

4 https://www.esma.europa.eu/sites/default/files/2025-09/ESMA50-1949966494-3846_TRV_2_2025.pdf (dernière version publiée le 18 novembre 2025).

5 *European Securities and Markets Authority*.

6 Niveau « rouge » (les deux niveaux inférieurs étant, par ordre décroissant d'importance, « orange » et « jaune »).

Ce document ne constitue ni une position, ni une recommandation. Les pratiques identifiées comme « bonnes » ou « mauvaises » soulignent des approches constatées lors des contrôles réalisés et susceptibles de favoriser ou de contrecarrer le respect de la réglementation applicable à la gestion des risques opérationnels. Les rappels réglementaires précisés dans les encadrés de la section 3 correspondent à des manquements identifiés au cours des contrôles des SGP du panel.

2- PERIMETRE

➢ Présentation de l'échantillon contrôlé

Le contrôle a été mené en parallèle sur cinq SGP, dont les principales caractéristiques sont présentées dans le tableau ci-après. Trois des SGP du panel (n°1 à 3) appartiennent à un groupe. Toutes disposent d'un agrément AIFM intégral.

SGP	n°1	n°2	n°3	n°4	n°5
Activités principales	Stratégies actions, obligataires, de trésorerie et *multi-assets*	*Stock picking* ciblant des petites et moyennes capitalisations de la zone Euro	Gestion traditionnelle via du *stock picking incluant des fonds structurés* sans effet de levier	Capital investissement dans le secteur de la santé	Gestion traditionnelle, fondée sur une approche de *stock picking (n'incluant pas de FIA)*
Clientèle	Professionnelle et non professionnelle	Professionnelle	Professionnelle et non professionnelle	Professionnelle	Non professionnelle
Effectifs (% de gérants)	200 < x (14 %)	10 < x < 50 (34,7 %)	10 < x < 50 (26 %)	100 < x < 200 (7 %)	10 < x < 50 (47 %)
Encours sous gestion collective (au 31 décembre 2024)					
Total (Mds€)	50 < x	1 < x < 5	1 < x < 5	1 < x < 5	x < 1
Nombre de fonds	50 < x	x < 10	5 < x < 30	5 < x < 30	5 < x < 30

Seules les SGP n°1 et 5 délèguent la gestion d'une partie de leurs fonds à une SGP externe (à hauteur de, respectivement, 1,7 % et 55,8 % de leurs encours).

➢ Thèmes de travail et méthodologie appliquée

Les contrôles ont porté sur la période allant du 1er janvier 2022 au 31 décembre 2024 et ont couvert :

- l'organisation et les moyens dédiés à l'identification, au suivi et à la gestion des risques opérationnels ;
- le corps procédural relatif à l'identification, au suivi et à la gestion de ces risques ;
- la mise en œuvre pratique du dispositif de collecte, d'analyse et d'instruction des incidents opérationnels ;
- les modalités de couverture des risques en matière de responsabilité professionnelle ;
- le *reporting* relatif aux incidents opérationnels auprès des instances dirigeantes et de l'AMF ;
- les travaux de contrôle interne mené sur le dispositif de gestion des risques opérationnels.

➢ Réglementation applicable

Les analyses menées se sont appuyées sur :

- le code monétaire et financier (« **CMF** ») ;
- le règlement général de l'AMF (« **RG AMF** ») ;
- le règlement délégué (UE) n° 231/2013 du 19 décembre 2012 (« **RD AIFM** ») ;
- le règlement délégué (UE) n°2017/565 du 25 avril 2016 (« **RD MIF II** ») ;
- le règlement européen n°2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (*digital operational resilience act* « **DORA** ») ;

- la position-recommandation AMF DOC-2012-19 : « *Guide d'élaboration du programme d'activité des sociétés de gestion de portefeuille et des placements collectifs autogérés* » ;
- la position-recommandation AMF DOC-2014-06 : « *Guide relatif à l'organisation de la gestion des risques, de la conformité et du dispositif de contrôle au sein des sociétés de gestion de portefeuille* » ;
- l'instruction DOC-2012-01 intitulée « *Organisation de l'activité de gestion de placements collectifs et du service d'investissement de gestion de portefeuille pour le compte de tiers en matière de gestion des risques* » ;
- d'autres éléments pertinents de la doctrine de l'AMF.

L'encadré ci-dessous inclut les principales sources de droit sur lesquelles l'AMF s'est appuyée pour réaliser ses travaux.

CADRE REGLEMENTAIRE

Concernant l'organisation et les moyens dédiés à l'identification, au suivi et à la gestion des risques opérationnels :

- **Articles 321-23 du RG AMF (OPCVM), 318-1 du RG AMF (FIA), 22 du RD AIFM (FIA) et 21 (1) du RD MIF II (gestion sous mandat - « GSM »)** concernant l'utilisation en permanence des moyens, notamment matériels, financiers et humains adaptés et suffisants ;
- **Articles L. 533-10 (4°) du CMF (GSM), 321-93 à 321-96 du RG AMF (OPCVM), 318-58 à 318-61 du RG AMF (FIA), 31 du RD MIF II (GSM), 4 de l'instruction DOC-2012-01 et position-recommandation AMF DOC-2012-19 (§ 3.2.8)** concernant les mesures raisonnables pour éviter une aggravation indue du risque opérationnel dans le cadre d'une externalisation ;
- **Articles 318-38 et 318-39 du RG AMF (FIA), 321-77 du RG AMF (OPCVM), 312-45 du RG AMF (GSM), articles 39 et 42 du RD AIFM (FIA), 23 (2) du RD MIF II (GSM) et 2 et 3 de l'instruction DOC-2012-01** concernant la mise en place d'une fonction de gestion des risques exercée de manière indépendante ;
- **Articles 321-77 et 321-81 du RG AMF (OPCVM), 39 du RD AIFM (FIA), 312-45 du RG AMF (GSM) et 7 de l'instruction DOC-2012-01** concernant les techniques et outils de mesure des risques ;
- **Instruction DOC-2012-01** concernant l'organisation de l'activité de gestion de placements collectifs et du service d'investissement de gestion de portefeuille pour le compte de tiers en matière de gestion des risques.

Concernant le corps procédural dédié à l'identification, au suivi et à la gestion des risques opérationnels :

- **Articles 321-76 du RG AMF (OPCVM), 12 du RD AIFM (FIA), 312-44 (§4) du RG AMF (GSM)** concernant la définition du risque opérationnel ;
- **Articles L. 532-9 du CMF, 321-4 du RG AMF (OPCVM) et 316-5 du RG AMF (FIA)** concernant la conformité du corps procédural avec le programme d'activité ;
- **Articles 321-30 du RG AMF (OPCVM), 61 (1) du RD AIFM (FIA) et 22 (1) du RD MIF II (GSM)** concernant l'établissement et maintien de politiques, procédures et mesures adéquates visant à détecter tout risque de non-conformité aux obligations professionnelles ;
- **Articles 321-78, 321-79 du RG AMF (OPCVM), 312-46 et 312-48 (I) du RG AMF, 13 (1), 40 du RD AIFM (FIA) et 23 (1) (a) du RD MIF (GSM)** concernant la politique de gestion des risques ;
- **Articles 321-35 (f) du RG AMF (OPCVM), 60 (2) (g) du RD AIFM (FIA), 25 (1) du RD MIF II (GSM)** concernant le réexamen périodique de la politique de gestion des risques par les instances dirigeantes ;
- **Articles 321-81 (OPCVM) et 312-48 (II) (GSM) du RG AMF, 45 (3) du RD AIFM (FIA) et article 5 de l'instruction DOC-2012-01** concernant la cartographie des risques ;
- **Articles 321-81 (I) (a) (OPCVM) et 312-48 (I) (GSM) du RG AMF, 40 (2) du RD AIFM (FIA), 5 de l'instruction DOC-2012-01** concernant la procédure mesurant les risques auxquels sont exposés les fonds ;
- **Articles 321-24 du RG AMF (OPCVM), 57 (2) du RD AIFM (FIA) et 21 (2) du RD MIF II (GSM)** concernant les systèmes et procédures permettant de sauvegarder la sécurité, l'intégrité et la confidentialité des informations ;

- **Articles 321-25 du RG AMF (OPCVM), 57 (3) du RD AIFM (FIA) et 21 (3) du RD MIF II (GSM)** concernant le plan de continuité des activités ;
- **Article 321-26 du RG AMF (OPCVM), 57 (4) du RD AIFM (FIA) et 21 (4) du RD MIF II (GSM))** concernant l'établissement de politiques et procédures comptables.

Concernant le processus de pilotage des risques opérationnels mis en œuvre :

- **Articles 321-80 du RG AMF (OPCVM), 312-47 et 312-48 (II) du RG AMF (GSM), 13 (5), (6), 41 et 60 (2) du RD AIFM (FIA), 23 (1) (c) du RD MIF II (GSM) et 6 de l'instruction DOC-2012-01** concernant l'évaluation, contrôle et réexamen périodique la politique de gestion des risques ;
- **Articles 321-23 (VII) du RG AMF (OPCVM), 57 (1) (e) du RD AIFM (FIA) et 21 (1) (f) du RD MIF II (GSM)** concernant l'enregistrement de manière adéquate et ordonnée du détail des activités et de l'organisation interne de la SGP ;
- **Article 13 (2), (3), (4) du RD AIFM** concernant l'enregistrement et suivi des dysfonctionnements opérationnels, pertes et dommages ;
- **Articles 321-40, 321-41 du RG AMF (OPCVM), 318-10 et 318-10-1 du RG AMF (FIA) et instruction recommandation AMF DOC 2012-07** concernant le traitement des réclamations ;
- **Position-recommandation AMF-DOC-2011-25 (section 4),** concernant l'indemnisation amiable des porteurs ;
- **Articles 317-2 (IV) du RG AMF, 12 (3), 14 et 15 du RD AIFM (FIA)** concernant les fonds propres supplémentaires et l'assurance de RCP ;
- **Articles 321-97 (OPCVM), 318-62 (I) (4) (5) (FIA) du RG AMF, 75 (f) du RD AIFM (FIA) et 31 (2) (e) du RD MIF II (GSM)** concernant la gestion adéquate des risques découlant de la délégation ;
- **Position-recommandation DOC-2012-19 (section 6.2)** concernant d'élaboration du programme d'activité des sociétés de gestion de portefeuille et des placements collectifs autogérés.

Concernant le dispositif de *reporting* aux instances dirigeantes et à l'AMF relativement aux incidents opérationnels :

- **Articles 321-23 (VI) du RG AMF (OPCVM), 57 (1) (d) du RD AIFM (FIA) et 21 (1) (e) du RD MIF II (GSM)** concernant l'établissement d'un système efficace de remontées hiérarchiques et de communication des informations à tous les niveaux pertinents ;
- **Articles 321-77 (III) (d), (e) du RG AMF (OPCVM), 312-45 (III) (d), (e) du RG AMF (GSM) et 39 (1) (d), (e) du RD AIFM** concernant le *reporting* au conseil d'administration et à la fonction de surveillance ;
- **Articles 318-6 du RG AMF (FIA) et 321-35 (g) (OPCVM)** du RG AMF concernant l'information de l'AMF sur les incidents opérationnels ;
- **Articles 321-75-1 (OPCVM) et 318-37-1 du RG AMF (FIA)** concernant le compte rendu des indemnisations et du non-respect des règles d'investissement des fonds ;
- **Article 110 et annexe IV du RD AIFM** concernant les *reportings* AIFM.

Concernant le dispositif de contrôle interne appliqué à l'identification, au suivi et à la gestion des risques opérationnels :

- **Articles 321-86 (OPCVM), 318-51 (FIA) du RG AMF, 61 (3) (c) du RD AIFM (FIA) et 22 (3) (d) du RD MIF II (GSM)** concernant la différence entre le contrôle interne et le contrôle de 1er niveau ;
- **Articles 321-23 (IV), 321-27, 321-31 et 321-32 du RG AMF (OPCVM), 57 (1) (c), (6), 61 (2) (3) du RD AIFM (FIA), 21 (1) (c), (5) et 22 (2) (3) (4) du RD MIF II (GSM)** concernant l'existence d'une fonction efficace de conformité et le contrôle interne ;
- **Articles 321-83 du RG AMF (OPCVM), 62 du RD AIFM (FIA) et 24 du RD MIF II (GSM)** concernant l'existence d'une fonction de contrôle périodique ;
- **Articles 321-32 (2) et 321-36 du RG AMF (OPCVM) et 60 (4) et 61 (3) (b) du RD AIFM (FIA) et 22 (2) (c) du RD MIF II (GSM)** concernant les rapports aux dirigeants relatifs à la conformité, à l'audit interne et à la gestion des risques.

3- CONSTATS ET ANALYSES

3.1. ORGANISATION ET MOYENS DEDIES A LA GESTION DES RISQUES OPERATIONNELS

Sur le panel de SGP contrôlées, la fonction en charge de la gestion des risques opérationnels apparaît dotée de moyens suffisants et compatibles avec le volume des incidents observés. Les dirigeants responsables de ces SGP sont régulièrement informés de la détection de ces derniers et de l'avancement de leur instruction au travers de comités existants.

3.1.1. Moyens humains

La fonction en charge de la gestion des risques opérationnels élabore notamment la cartographie des risques opérationnels et assure la collecte, l'instruction, le suivi et le reporting relatifs aux incidents opérationnels.

Dans la majorité des SGP du panel (n°1 à 4), cette fonction est exercée par le responsable de la conformité et du contrôle interne (« **RCCI** »). Dans la SGP n°5 en revanche, elle est dévolue au responsable du contrôle des risques. Dans l'ensemble des SGP analysées, elle bénéficie d'un rattachement direct à un dirigeant responsable[7]. Dans la SGP n°5, un dirigeant responsable exerce d'ailleurs cette fonction à hauteur de 20 % de son temps de travail.

La personne en charge de la gestion des risques opérationnels s'appuie sur une équipe d'une à trois personnes au sein des SGP n°2 à 5. Cet effectif atteint une quarantaine de personnes dans la SGP n°1 (qui dispose d'un personnel sensiblement plus nombreux) subdivisé en deux équipes dont l'une est dédiée aux risques opérationnels non informatiques et l'autre aux risques technologiques[8] et de rupture de continuité d'activité. Le niveau d'expérience moyen de ces ressources en matière de gestion des risques opérationnels dans le secteur de la gestion d'actifs est supérieur à 5 ans. Aucune externalisation n'a été constatée sur ce périmètre pour les cinq SGP du panel.

Seules trois des cinq SGP du panel (n°1, 2 et 4) ont organisé des formations relatives à la gestion du risque opérationnel, à l'intention de l'ensemble de leur personnel, sur la période analysée. Ces formations ont ciblé la prévention de la fraude externe et interne (au sein de la SGP n°1, en 2022 et 2024) ainsi qu'une présentation du dispositif de gestion des incidents opérationnels en termes d'identification, de collecte et d'escalade (au sein des SGP n°2 et 4). Cette seconde formation a lieu semestriellement au sein de la SGP n°2. Elle a été délivrée pour la première fois en avril 2025 par la SGP n°4.

Toutes les SGP du panel ont, en revanche, proposé à leurs effectifs une sensibilisation aux risques d'origine cyber. Cette dernière a pris la forme de tests de *phishing*[9] au sein des SGP n°2 et 4.

3.1.2. Moyens techniques

Seule la SGP n°1 a déployé deux outils informatiques spécifiques dédiés à la collecte des incidents opérationnels (registre interne) et d'origine cyber (application externe). Les quatre autres SGP utilisent dans ce cadre les outils bureautiques usuels, les plans de remédiation décidés à la suite des incidents opérationnels constatés étant suivis au sein d'une solution collaborative standard du marché.

La SGP n°2 envisageait une migration avant la fin de l'exercice 2025 vers le registre informatisé des incidents opérationnels de son groupe d'appartenance.

---

7 Au sens de l'article L. 532-9 II 4° du CMF et de l'article 317-5 du RG AMF.

8 Il s'agit des risques informatiques (tels qu'une panne) et de cybersécurité (différents des précédents en ce qu'ils induisent une intention de nuire).

9 Test destinés à vérifier le niveau de vigilance des collaborateurs dans le traitement des courriels pouvant contenir des liens malveillants.

3.1.3. Gouvernance

Les cinq SGP du panel prévoient le pilotage du dispositif de gestion des risques opérationnels via un comité en place au sein de leur dispositif de gouvernance. Le rôle de ce comité est d'assurer le suivi des indicateurs de risque au regard des limites définies comme acceptables. Dans ce cadre, les incidents opérationnels survenus au cours de la période écoulée y sont présentés, ainsi que leurs conséquences, et l'état d'avancement des plans de remédiation est mis en regard.

SGP	n°1	n°2	n°3	n°4	n°5
Instance	comité des risques du groupe comité des risques opérationnels de la SGP	comité de direction	comité des risques	comité de contrôle et risques	comité des risques
Fréquence	mensuelle semestrielle	hebdomadaire	mensuelle	deux fois par an	trimestrielle
Composition sélective	Dirigeant responsable, directeur des risques, RCCI, directeur de l'audit interne Responsable des risques opérationnels, responsable du middle-office, responsable des risques, RCCI	Dirigeant responsable, secrétaire général, responsable de la gestion, responsable du middle-office, responsable des risques, RCCI	Dirigeants responsables, équipes de gestion, responsable des risques, RCCI	Dirigeants responsables, RCCI, responsable des risques	Dirigeants responsables (dont le responsable des risques), directeurs généraux délégués, RCCI

Seule la SGP n°1 a déployé deux instances sur ce périmètre, l'une au niveau du groupe et l'autre au niveau de la filiale (SGP). Dans ce cadre, le comité des risques du groupe délègue au comité des risques opérationnels de la SGP le suivi des incidents résultant de la défaillance des processus opérationnels de cette dernière, ainsi que le suivi de la mise en œuvre des mesures de renforcement de ces processus. Le support de ce second comité propose une décomposition des incidents opérationnels subis au cours du trimestre écoulé par département. Il fournit également un suivi des mises à jour récentes de la cartographie des risques et du corps procédural.

De plus, cette SGP (n°1) assure le suivi des risques informatiques, d'origine cyber et de rupture d'activité au sein d'un comité dédié qui se réunit au moins quatre fois par an suivant une composition équivalente à celle du comité des risques du groupe (signalée dans le tableau *supra*), complétée par un directeur dédié à ce type de risque. Dans le cadre de l'entrée en application de la règlementation DORA[10] le 17 janvier 2025, cette SGP a également mis en place un comité dédié au pilotage de ses prestataires externes en technologie de l'information et de la communication (« **TIC** »), importants ou sensibles. Ce comité se réunit toutes les deux semaines sous la présidence du responsable de la sécurité des systèmes d'information (« **RSSI** »).

Bonnes pratiques :

- Proposer, sur une fréquence annuelle, une formation à l'ensemble du personnel visant les modalités d'identification, de collecte et d'escalade des incidents opérationnels.
- Inclure, dans le support du comité périodique de suivi des risques opérationnels, un focus sur les mises à jour significatives opérées tant sur la cartographie de ces risques que dans le corps procédural.

3.2. CORPS PROCEDURAL DEDIE A LA GESTION DES RISQUES OPERATIONNELS

Les corps procéduraux consultés présentent, en majorité, le processus d'évaluation des risques et d'instruction des incidents opérationnels de manière claire, ainsi que son lien avec le processus de traitement des réclamations. En revanche, les modalités de comptabilisation (et de vérification *a posteriori*) des pertes associées à ces incidents

[10] Cf. « cadre règlementaire » dans la section 2 *supra*.

sont moins bien couvertes, de même que les règles de calcul des fonds propres supplémentaires utilisables (règlementairement) afin de couvrir les risques en matière de responsabilité pour négligence professionnelle.

3.2.1. Définition des concepts fondamentaux

- Risque opérationnel

Les cinq SGP du panel ont formalisé de manière précise leur définition du risque opérationnel au sein de leur corpus procédural, qui est fidèle à celle prévue par la réglementation.

- Incident opérationnel

Quatre des cinq SGP du panel (n°1 à 4) ont formalisé dans ce corpus une définition de l'incident opérationnel. Ces définitions convergent dans le sens d'un événement inattendu, matérialisant un risque opérationnel, et résultant d'une anomalie, d'une défaillance, d'une inadaptation ou d'un événement extérieur. Trois SGP (n°1 à 3) y intègrent la notion d'impact financier (positif, négatif ou nul), voir non financier pour la SGP n°2. En revanche, le corps procédural de la SGP n°5 ne définit pas la notion d'incident opérationnel.

- Appétit pour le risque opérationnel (*operational risk appetite*)

Il s'agit du niveau maximal d'impact, en termes de risque opérationnel, que la SGP estime être en capacité de supporter dans la conduite de ses activités (coûts de remédiation post-incidents inclus). Seules trois des cinq SGP du panel (n°1, 2 et 5) l'ont formalisé au sein de leur corps procédural :

- la SGP n°1 l'a défini de manière chiffrée et fait valider par son organe délibérant à hauteur de 3,5 M€ ;
- la SGP n°2 a repris le seuil de son groupe qui est nul pour les risques opérationnels ;
- la SGP n° 5 définit le seuil de l'exercice N+1 (*a posteriori*) comme égal au montant total des pertes dues à des incidents opérationnels constatées sur l'exercice N (soit 10,5 k€ pour l'exercice 2024).

Sur le périmètre des risques informatiques, la SGP n°1 a défini son appétit pour le risque au travers de plusieurs indicateurs parmi lesquels figurent le pourcentage de postes de travail bénéficiant d'un antivirus renforcé (seuil minimum : 95 %), le taux de disponibilité de l'environnement de production (seuil minimum : 98 %) et la proportion des infrastructures obsolètes (seuil maximum : 5 %).

3.2.2. Cartographie des risques opérationnels

Les cinq SGP du panel disposent d'une cartographie des risques formelle, régulièrement mise à jour et validée par l'organe de direction.

Pour les SGP n°1 à 4, les risques opérationnels sont suivis au sein de la cartographie globale, soit via une rubrique spécifique, soit via un suivi de risques plus granulaires (fraude, transaction erronée, échec de sauvegarde informatique par exemple).

La SGP n°5, quant à elle, a mis en place une cartographie spécifiquement dédiée aux risques opérationnels qu'elle catégorise en sept familles : « 1. Fraude interne » ; « 2. Fraude externe » ; « 3. Pratique en matière d'emploi et de sécurité sur le lieu de travail » ; « 4. Clients, produits et pratiques commerciales » ; « 5. Dommages aux actifs corporels » ; « 6. Interruptions d'activité et dysfonctionnements des systèmes » et « 7. Exécution, livraison et gestion des processus ».

S'agissant du risque d'origine cyber, il est pris en compte par les cinq SGP du panel dans leur cartographie des risques respective, par exemple sous la dénomination « interruptions de l'activité et dysfonctionnement des systèmes » au sein des SGP n°1 et 5.

Les cartographies des risques consultées distinguent, pour les cinq SGP du panel, la notion de risque « brut » de celle de risque « net ». Les SGP contrôlées incluent, dans l'évaluation du second, l'analyse des incidents opérationnels subis et les résultats des travaux de contrôle interne exécutés, processus par processus.

Quatre des cinq SGP (n°1, 2, 3 et 4) ont formalisé une grille d'évaluation formelle des risques opérationnels définis dans la cartographie. Les SGP n°1, 2 et 4 réalisent cette évaluation tant sur les impacts financiers que non financiers (exemple : impact règlementaire, réputationnel, juridique) via plusieurs niveaux de gravité (faible, moyen, fort, par exemple). S'agissant des risques d'origine cyber, la SGP n°1 applique la grille d'évaluation de son groupe qui évalue à un niveau « significatif », par exemple, la fuite massive de données confidentielles ou une attaque touchant un fournisseur externe et impactant – par rebond – l'activité de la SGP.
La SGP n°3 procède de même mais sur la seule dimension financière. Elle considère ainsi une perte supérieure à 300 k€ comme majeure, modérée si elle est comprise entre 150 et 300 k€ et mineure si elle est inférieure à 150 k€. En revanche, la SGP n°5 n'a pas formalisé de méthode de cet ordre, l'évaluation des impacts des incidents opérationnels subis étant réalisés au cas par cas, à dire d'expert, par le responsable des risques.

3.2.3. Corpus procédural relatif à la gestion des risques et des incidents opérationnels

Pour les cinq SGP du panel, les documents procéduraux examinés définissent notamment l'organisation et la gouvernance du dispositif de gestion des risques opérationnels (analysées dans la section 3.1 *supra*), les modalités d'identification, d'instruction et d'escalade des incidents, les mécanismes de *reporting* aux instances dirigeantes ainsi que le dispositif de contrôle interne applicable. Chez la SGP n° 3, ce corpus inclus un arbre de décision illustrant le processus de traitement des incidents opérationnels, les interactions entre les parties prenantes et les outils utilisés. En revanche, la SGP n'a formalisé que tardivement (octobre 2023) les règles de gestion procédurales des risques opérationnels, celles-ci demeurant en outre laconiques en ce qui concerne le traitement des incidents subis.

La comptabilisation des pertes générées par les incidents opérationnels subis, ainsi que les modalités du rapprochement effectué *a posteriori* entre les données comptables et celles de la base des incidents, sont encadrées par une procédure dans deux SGP du panel (n°1 et 3). En revanche, ces règles n'ont pas fait l'objet d'une procédure formalisée au sein des SGP n°4 et 5. Elles demeurent lacunaires dans la procédure comptable de la SGP n°2, qui a, de surcroît, été mise en œuvre tardivement[11].

En outre, seules trois des cinq SGP du panel (n°2, 4 et 5) disposent d'une procédure encadrant le calcul des fonds propres réglementaires. De plus, les règles de calcul des fonds propres supplémentaires pouvant être utilisés par les SGP - agréées au sens de la directive AIFM - pour se couvrir au regard des risques en matière de responsabilité professionnelle ne sont pas explicitées dans la procédure de la SGP n°4.

Par ailleurs, quatre SGP du panel (n°1, 3, 4 et 5) se sont dotées de procédures dédiées définissant les modalités d'identification, de collecte et de traitement des réclamations, ce qui n'est pas le cas de la SGP n°2. Les SGP n°4 et 5 prévoient explicitement, dans leur procédure respective, d'analyser les réclamations reçues à l'aune des incidents opérationnels subis afin d'en identifier d'éventuelles causes partagées.

Enfin, les cinq SGP contrôlées disposent d'une procédure d'encadrement des relations avec les prestataires externes importants ou sensibles. Ces procédures signalent la prise en compte des risques opérationnels associés au service rendu lors des étapes de sélection[12] et de suivi de ces prestataires, ainsi que durant la phase de

[11] Décembre 2024.
[12] Celle-ci s'articule autour de critères tels que l'existence d'une procédure de gestion des risques opérationnels, d'un plan de continuité d'activité et d'un dispositif robuste de gestion des risques d'origine cyber et de traitement des données confidentielles.

contractualisation[13]. En l'absence de critères précis d'appréciation de la qualité de service, la procédure de la SGP n°5 demeure toutefois peu opérationnelle.
S'agissant du pilotage des risques opérationnels liés à la gestion déléguée à une SGP tierce, elle fait l'objet d'une procédure dédiée au sein de la SGP n°1, mais pas de la SGP n°5 (les 3 autres n'étant pas concernées).

3.2.4. Capacité à exécuter le contrôle des risques opérationnels en situation dégradée

Seul le plan de continuité d'activité (« **PCA** ») mis en place par la SGP n°1 couvre de manière satisfaisante les moyens requis pour la gestion des risques opérationnels. Il se réfère à la réglementation DORA et présente les modalités de reprise d'activité au regard des différents scénarios de crise envisagés (exemple : indisponibilité de l'environnement de travail local).

En revanche, le PCA des quatre autres SGP du panel (n°2 à 5) ne couvre que partiellement le dispositif de gestion des risques opérationnels. En effet, celui de la SGP n°2 omet de prévoir un *backup* pour le RCCI, en dépit du rôle central de ce dernier dans le dispositif cité. Quant à celui des SGP n°3, 4 et 5, il n'identifie pas les activités critiques de la SGP (exemple : transmission d'ordres, valorisation), ni n'établit de hiérarchie claire de reprise d'activité.

De plus, seule la SGP n°1 a testé son PCA de manière satisfaisante au cours de la période sous contrôle. Les exercices menés (et dûment formalisés) ont porté sur la capacité du personnel à travailler à distance et sur la bascule des installations informatiques principales (*datacenter*) vers le *datacenter* de secours. Les SGP n°2, 3 et 5 n'ont réalisé aucun test de cet ordre. Quant à la SGP n°4, elle n'a pas testé conjointement, sur une base annuelle, sa capacité à restaurer ses données sensibles et à placer l'ensemble de son personnel en télétravail, en contradiction avec les exigences de son PCA.

3.2.5. Conformité du corps procédural analysé avec le programme d'activité

Le corps procédural analysé est conforme au programme d'activité de deux des cinq SGP du panel (n°1 et 2). Des divergences mineures ont été constatées pour les SGP n°3 (s'agissant de la souscription par la SGP d'une assurance RCP), 4 et 5 (s'agissant de la fréquence signalée de mise à jour de la politique et de la cartographie des risques opérationnels).

Rappels réglementaires en lien avec les manquements constatés lors des contrôles :

Concernant la conformité du corps procédural avec le programme d'activité :

- **Article L. 532-9 du CMF :** « *[…] (II) […] Les sociétés de gestion de portefeuille doivent satisfaire à tout moment aux conditions de leur agrément. […]* ».

Concernant le corps procédural dédié au dispositif de gestion des risques opérationnels :

- **Article 321-30 du RG AMF (OPCVM)** : « *La société de gestion de portefeuille établit et maintient opérationnelles des politiques, procédures et mesures adéquates visant à détecter tout risque de non-conformité aux obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier ainsi que les risques en découlant et à minimiser ces risques […].*» **(et article 61 (1) du RD AIFM (FIA), 22 (1) du RD MIF II) ;**
- **Article 321-78 du RG AMF (OPCVM)** : « *I. - La société de gestion de portefeuille établit, met en œuvre et garde opérationnelle une politique de gestion des risques appropriée et documentée qui permet de déterminer les risques auxquels les OPCVM qu'elle gère sont exposés ou pourraient être exposés. […]*

[13] Celle-ci s'articule autour de clauses telles que le devoir d'information de la SGP en cas de survenance de tout évènement susceptible d'impacter sensiblement la qualité et la continuité de l'externalisation, l'obligation pour le prestataire de disposer d'une assurance, le droit pour la SGP de réaliser des audits (pour les prestations essentielles seulement) et le droit de regard de l'AMF.

II. - La politique de gestion des risques comporte toutes les procédures nécessaires pour permettre à la société de gestion de portefeuille d'évaluer, pour chaque OPCVM qu'elle gère, l'exposition de cet OPCVM aux risques de marché, de liquidité et de contrepartie, ainsi que l'exposition des OPCVM à tout autre risque, y compris le risque opérationnel, susceptible d'être significatif pour les OPCVM qu'elle gère.

III. - La politique de gestion des risques doit porter au moins sur les éléments suivants : a) les techniques, outils et dispositions qui leur permettent de se conformer aux obligations énoncées aux articles 321-81, 411-72 et 411-73 ; b) l'attribution des responsabilités en matière de gestion des risques au sein de la société de gestion de portefeuille. […].» **(et articles 13 (1), 40 (1) (3), 45 du RD AIFM, 312-46 (I) (II) (III) (a) (b) du RG AMF (GSM)) ;**

- **Article 321-79 du RG AMF (OPCVM)** : « *La société de gestion de portefeuille établit, met en œuvre et maintient opérationnelles une politique et des procédures de gestion des risques efficaces, appropriées et documentées qui permettent d'identifier les risques liés à ses activités, processus et systèmes et, le cas échéant, de déterminer le niveau toléré par elle.* » **(et articles 13 (5), 40 (2) du RD AIFM, 23 (1) (a) du RD MIF II, 312-46 du RG AMF (GSM)).**

Concernant le corps procédural relatif aux fonds propres supplémentaires :

- **Article 12 (3) du RD AIFM :** *« 3. Les risques en matière de responsabilité professionnelle sont couverts à tout moment, soit par des fonds propres supplémentaires appropriés dont le montant est déterminé conformément à l'article 14, soit par un niveau approprié de couverture par une assurance de responsabilité civile professionnelle, déterminé conformément à l'article 15* » ;
- **Article 14 du RD AIFM (FIA)** : « *[…] (2) Afin de couvrir les risques en matière de responsabilité pour négligence professionnelle, le gestionnaire fournit des fonds propres supplémentaires* ***s'élevant au moins à 0,01 % de la valeur des portefeuilles des FIA gérés****. La valeur des portefeuilles des FIA gérés correspond à la somme de la valeur absolue de tous les actifs détenus par tous les FIA gérés par le gestionnaire, y compris les actifs acquis grâce à l'effet de levier, les instruments dérivés étant alors évalués à leur valeur de marché (3) L'exigence de fonds propres supplémentaires définie au paragraphe 2 est recalculée à la fin de chaque exercice et le montant de fonds propres supplémentaires est ajusté en conséquence. Le gestionnaire établit, met en œuvre et applique des procédures afin de suivre en permanence la valeur des portefeuilles des FIA gérés, calculée conformément au second alinéa du paragraphe 2. Si avant le recalcul annuel mentionné au premier alinéa, la valeur des portefeuilles des FIA gérés augmente sensiblement, le gestionnaire recalcule dans les meilleurs délais l'exigence de fonds propres supplémentaires et ajuste en conséquence le montant de ces derniers. […]* » ;
- **Position-recommandation AMF DOC-2012-19, paragraphe 6.2.1 :** « *[…] le taux de 0.01 % évoqué au paragraphe 2 de l'article 14 du règlement délégué (UE) n° 231/2013 de la Commission du 19 décembre 2012* ***est un taux minimum****. Conformément aux dispositions précitées, le taux retenu par la société de gestion de portefeuille doit résulter d'une analyse menée régulièrement par cette dernière concernant les risques qu'elle supporte et leur quantification. Le montant ainsi défini doit correspondre aux risques supportés et être d'un niveau suffisant pour permettre de prendre les mesures de remédiations rendues nécessaires (ex : couvrir au minimum les frais juridiques et de procédure).* ***L'analyse doit être formalisée et les hypothèses justifiées et historisées*** ».

Concernant l'existence d'une procédure comptable :

- **Article 321-26 du RG AMF (OPCVM)** : « *La société de gestion de portefeuille établit et maintient opérationnelles des politiques et procédures comptables qui lui permettent de fournir en temps utile, à la requête de l'AMF, des informations financières qui offrent une image fidèle et sincère de sa situation financière et qui sont conformes à toutes les normes et règles comptables en vigueur. »* **(et articles 57 (4) du RD AIFM (FIA) et 21 (4) du RD MIF II (GSM)).**

Concernant l'existence d'une procédure encadrant le traitement des réclamations :

- **Article 321-40 du RG AMF (OPCVM) :** « *I. - La société de gestion de portefeuille établit et maintient opérationnelle une procédure efficace et transparente en vue du traitement raisonnable et rapide des réclamations adressées par l'ensemble des porteurs de parts ou actionnaires d'OPCVM […]. Les informations sur la procédure de traitement des réclamations sont mises gratuitement à la disposition des porteurs de parts ou actionnaires. La procédure de traitement des réclamations est proportionnée à la taille et à la structure de la société de gestion de portefeuille.* » **(et articles 318-10 du RG AMF (FIA), 26 (1) du RD MIF II) ;**
- **Article 321-41 du RG AMF (OPCVM)** : « *La société de gestion de portefeuille prend des mesures conformément à l'article 411-138 et établit des procédures et des modalités appropriées afin de garantir qu'elle traitera correctement les réclamations des porteurs de parts ou actionnaires d'un OPCVM et que ceux-ci ne sont pas limités dans l'exercice de leurs droits lorsqu'ils résident dans un autre État membre de l'Union européenne ou État partie à l'Espace économique européen. Ces mesures permettent aux porteurs de parts ou actionnaires d'un OPCVM d'adresser une réclamation dans la langue officielle ou dans l'une des langues officielles de l'État dans lequel l'OPCVM est commercialisé et de recevoir une réponse dans la même langue. La société de gestion de portefeuille établit également des procédures et des modalités appropriées pour fournir des informations, à la demande du public, ou, lorsqu'elle gère un OPCVM établi dans un autre État de l'Union européenne ou État partie à l'Espace économique européen, des autorités compétentes de l'État membre d'origine de cet OPCVM. Ces dispositions s'appliquent lorsqu'aucun service d'investissement n'est fourni à l'occasion de la souscription.* » **(et articles 318-10-1 du RG AMF (FIA), 26 (2) et suivants du RD MIF II).**

Concernant l'encadrement des activités externalisées :

- **Article 321-93 du RG AMF (OPCVM) :** « *Lorsque la société de gestion de portefeuille confie à un tiers l'exécution de tâches ou fonctions opérationnelles essentielles ou importantes pour la fourniture d'un service ou l'exercice d'activités, elle prend des mesures raisonnables pour éviter une aggravation indue du risque opérationnel.* » **(et articles 318-58 du RG AMF (FIA), 31 (1) du RD MIF II).**

Concernant la capacité à exécuter le contrôle des risques opérationnels en situation opérationnelle dégradée

- **Article 321-25 du RG AMF (OPCVM) :** « *La société de gestion de portefeuille établit et maintient opérationnels des plans de continuité de l'activité afin de garantir, en cas d'interruption de ses systèmes et procédures, la sauvegarde de ses données et fonctions essentielles et la poursuite de son activité de gestion d'un OPCVM ou, en cas d'impossibilité, afin de permettre la récupération en temps utile de ces données et fonctions et la reprise en temps utile de ses activités.* » **(et articles 57 (3) du RD AIFM (FIA), 21 (3) du RD MIF II (GSM)).**

Bonnes pratiques :

- Définir *ex ante*, formellement et de manière chiffrée, l'appétit pour le risque opérationnel de la SGP en relation avec le niveau de pertes (et de dépenses de remédiation) qu'elle juge supportable au regard de son dispositif de contrôle des risques et de ses fonds propres.
- Définir un appétit pour le risque informatique en s'appuyant sur des indicateurs pratiques tels que le pourcentage de postes de travail bénéficiant d'un antivirus renforcé ou le taux de disponibilité de l'environnement de production.
- Formaliser une cartographie dédiée aux risques opérationnels, distincte de la cartographie générale des risques.
- Dissocier, dans la cartographie des risques opérationnels, le risque « brut » du risque « net » en incluant, dans l'évaluation du second, l'analyse des incidents opérationnels subis et les résultats des travaux de contrôle interne exécutés, processus par processus.

- Mettre en place, au sein du corps procédural, un arbre de décision schématisant de manière claire le processus de traitement d'un incident opérationnel et les règles d'escalade associées en fonction de son niveau de gravité.
- Définir, au sein du corpus procédural, des critères précis de sélection des prestataires et établir une liste des clauses minimales devant figurer dans les contrats d'externalisation, afin de sécuriser la relation et de maîtriser les risques opérationnels associés.

Mauvaises pratiques :

- Définir l'appétit pour le risque opérationnel *a posteriori* et sur la seule base des incidents opérationnels subis au cours de l'exercice écoulé.
- Ne pas inclure à la cartographie des risques opérationnels une grille d'évaluation graduelle des impacts financiers et non financiers de ces risques.

3.3. PROCESSUS DE PILOTAGE DES RISQUES OPERATIONNELS MIS EN OEUVRE

L'ensemble des SGP du panel ont mis en place un registre informatique de collecte des incidents opérationnels. Bien que les registres en place permettent un suivi satisfaisant du niveau de risque opérationnel auquel ces SGP ont été soumises au cours de la période sous contrôle, des améliorations sont possibles s'agissant notamment de l'évaluation systématique du niveau de gravité des évènements constatés, ainsi que du suivi des plans de remédiation décidés en regard.
Les volumétries constatées d'incidents opérationnels apparaissent cohérentes avec la taille et les stratégies de gestion des SGP contrôlées. La majorité d'entre eux concerne le processus de passation et d'exécution des ordres.

3.3.1. Registre des incidents opérationnels

Les cinq SGP du panel ont mis en place un registre informatique de collecte des incidents opérationnels, alimenté par la fonction en charge[14] de la gestion de ces derniers. A titre d'exemple, celui de la SGP n°3 se présente sous la forme d'un tableau Excel composé de neuf rubriques : « (1) Type de risque », « (2) Type d'incident », « (3) Date de l'événement », « (4) Date d'identification », « (5) Instrument », « (6) Description des faits », « (7) Causes », « (8) Impacts » et « (9) Plan d'actions ».

En revanche, ce registre n'a été mis en place que de manière tardive par les SGP n°4 et 5 (à savoir en 2023). Par ailleurs, celui de la SGP n°2 a fait l'objet, entre 2022 et 2023, d'un changement de la méthode d'évaluation des impacts des incidents qui n'est pas explicité. Il s'agit en l'espèce d'une évolution de 3 à 4 niveaux d'évaluation[15] sans précision d'une règle de correspondance entre la nouvelle et l'ancienne méthode.

Concernant enfin la SGP n°1, elle a communiqué deux registres ciblant respectivement les incidents opérationnels identifiés et les plans d'actions mis en œuvre en regard. Il s'avère cependant que le premier registre omet des incidents significatifs (exemple : intrusion physique dans les locaux) pourtant cités au sein du comité des risques opérationnels de la SGP[16]. Il ne permet pas non plus d'identifier les incidents qui ont été relevés par un tiers externe (exemple : dépositaire), alors que cette information fait l'objet d'un champ dédié dans les fiches d'instruction des incidents (« fiche incident »).

[14] Cf. section 3.1.1 *supra*.
[15] L'évolution de méthode d'évaluation a consisté à passer de {« acceptable », « fâcheux » et « grave »} à {1- faible, 2- modéré, 3- élevé et 4- très élevé}.
[16] Cf. section 3.1.3 *supra*.

Quant au second registre, il ne couvre que 30 % des incidents opérationnels pour lesquels des actions de remédiation sont demandées dans la première base. La SGP n°1 a expliqué cet écart en précisant que le second registre ne contenait que les plans d'actions suivis en direct par le responsable des risques opérationnels, à l'exclusion des plans affectés aux lignes métier.

La mission a procédé à une analyse comparative du contenu des registres sur les trois exercices de la période sous revue.

	exercice	SGP n°1	SGP n°2	SGP n°3	SGP n°4	SGP n°5
Nombre d'incidents recensés	2022	218	19	11	**Absence du registre**	**Absence du registre**
	2023	245	19	3	13	1
	2024	179	18	5	13	11
Evaluation dans le registre des niveaux de gravité des incidents collectés	2022	**Non réalisée**	1 « grave », 4 « fâcheux » et 14 « acceptables »	**Non réalisée**	**Absence du registre**	**Absence du registre**
	2023	**Non réalisée**	Tous classés comme « non significatifs »	**Non réalisée**	9 « Importants » et 4 « Mineurs »	**Non réalisée**
	2024	**Non réalisée**	Tous classés comme « non significatifs »	**Non réalisée**	**Non réalisée**	**Non réalisée**
Perte totale enregistrée (k€)	2022	3 800	néant	6,6	**Absence du registre**	**Absence du registre**
	2023	8 100	néant	< 1	néant	< 1
	2024	5 000	néant	5,3	4,6	10,5
Exemple d'incidents notables	2022	Exécution, livraison et gestion des processus	Renouvellement (automatique mais non désiré) d'un contrat de recherche Echec d'une transaction pour cause de non-référencement chez le dépositaire Dépassements actifs d'un ratio d'investissement	Erreurs de *booking* Erreurs de paramétrage des frais Erreurs d'exécution	Factures non comptabilisées	Erreur de bourse Incident de VL
	2023					
	2024					

Focus sur les incidents opérationnels significatif constatés au cours de la période sous contrôle

Au sein de la SGP n°2 en 2022 :

L'incident qualifié de « grave » lors de cet exercice 2022 a concerné le passage d'un ordre de vente sur une quantité d'actions supérieure au nombre réel détenu par les fonds, suivi d'une suspension d'ordre (vente à découvert). L'ordre a été suspendu dans des délais courts et les titres vendus à découvert ont été rachetés. Le logiciel de passation des ordres a fait l'objet d'une évolution informatique afin de réduire le risque de reproduction d'un tel incident.

Cet incident « grave » a généré un manque à gagner et non une perte avérée comptabilisée. En effet, il n'a pas occasionné de dépense supplémentaire des fonds concernés, ni de la SGP (de sorte qu'il n'a pas fait l'objet d'une comptabilisation). Son impact est en outre inférieur au seuil de matérialité retenu pour les fonds en matière d'indemnisation, tel que précisé dans le corps procédural de la SGP, soit 0,2 % de l'actif net de l'OPC.

S'agissant des quatre incidents qualifiés de « fâcheux » sur ce même exercice, il s'agit de trois erreurs dans le calcul de la valeur liquidative (« **VL** ») de fonds, et d'une interruption non souhaitée de l'envoi de transactions passées dans l'outil de passation des ordres vers la table de négociation du groupe (sans impact sur la VL des fonds).

Au sein de la SGP n°4 en 2023 :
Les 9 incidents opérationnels qualifiés d'importants concernent des erreurs commises par le prestataire en charge de la fonction externalisée de *middle-office*. Ces anomalies ont concerné le traitement des opérations sur titres (« OST ») et des appels de fonds, la comptabilité des fonds ainsi que des retards dans le calcul des VL des fonds.

- Suivi dédié aux incidents d'origine cyber

Ces incidents sont clairement identifiables dans les outils de suivi de quatre des cinq SGP du panel. Cette identification est permise, soit par leur suivi au sein d'un registre distinct (pour les SGP n°1 et 4), soit par l'usage d'un champ dédié au sein du registre global (pour les SGP n°2 et 5).

Exercice concerné	Nombre et nature des incidents d'origine cyber				
	SGP n°1	SGP n°2	SGP n°3	SGP n°4	SGP n°5
2022	942 (dont 97 critiques)	2 tentatives (avortées) de *phishing*	**Non suivi**	2 (détection d'un fichier malicieux sur le réseau et fuite de données)	Néant
2023	681 (dont 74 critiques)	1 tentative (avortée) de *phishing*	**Non suivi**	1 (exposition d'adresses personnelles)	Néant
2024	724 (dont 74 critiques)	Néant	**Non suivi**	18 (tentatives de *phishing*, connexion suspecte au réseau)	1 usurpation d'identité

Les incidents d'origine cyber constatés par la SGP n°1 ont principalement ciblé le code de certaines applications (à hauteur de 21,6 %), les prestataires informatiques externes (13,3 %) et l'infrastructure informatique (11,6 %). En revanche, les incidents d'origine cyber (et informatique) ne sont pas recensés par la SGP n°3, mais uniquement par son groupe d'appartenance (en charge de la maintenance du système d'information global).

Par ailleurs, la mission de contrôle a constaté l'usage par la SGP n°4 de quatre registres non harmonisés de suivi des incidents opérationnels. Ces derniers couvrent respectivement les incidents opérationnels (hors informatique et cyber), les incidents d'origine cyber, les incidents informatiques et ceux spécifiques au déploiement (récent) de l'outil de gestion de la relation client. Cette fragmentation des bases d'incidents **complexifie leur pilotage global du dispositif et menace la qualité du *reporting* associé (auprès des dirigeants et de l'AMF).**

- Analyse consolidée des causes des incidents opérationnels subis

Une telle analyse est réalisée *a posteriori* par trois SGP du panel (n°1, n°2 et 4). La SGP n°1 formalise cette analyse sous la forme d'un « *risks dashboard* » transmis régulièrement à ses dirigeants. Quant à la SGP n°4, le constat d'incidents récurrents constatés sur la prestation de *middle office* rendue par un prestataire externe[17] l'a conduite à dénoncer le contrat associé en décembre 2024.
En revanche, les SGP n° 2 et 4 n'ont pas formalisé ce suivi dans le cadre d'un support particulier mais ont initié des actions concrètes relevant principalement de la gestion de leur relation avec leurs prestataires.

3.3.2. Test du processus de gestion des risques opérationnels

La mission de contrôle a souhaité vérifier la robustesse du processus d'instruction des incidents opérationnels au travers d'un échantillon de ces derniers sélectionné dans les registres fournis (hors incidents d'origine cyber). Pour

[17] Cf. encadré *supra*.

chacun d'entre eux, la mission a demandé à la SGP de lui communiquer les fiches d'instruction produites en regard. L'objectif du test était de vérifier que chaque incident sélectionné avait fait l'objet d'une fiche formalisée et structurée, datée et signée, présentant le problème rencontré, estimant sa gravité et proposant des actions de remédiation.

SGP	n°1	n°2	n°3	n°4	n°5
Echantillon analysé (% du total des incidents opérationnels enregistrés)	1,5 %	12,5 %	100 %		
Résultat du test	EFFECTIF	PARTIELLEMENT EFFECTIF	PARTIELLEMENT EFFECTIF	INEFFECTIF	EFFECTIF

La mission de contrôle a constaté quelques défauts de traitement de ces fiches au sein des SGP n°2 et 3, par exemple une absence ponctuelle de signature du valideur. Elle constate en revanche qu'aucun des incidents du panel testé n'a fait l'objet d'une instruction formalisée par la SGP n°4.

- Enregistrements comptables des pertes liées aux incidents opérationnels subis

Trois des cinq SGP du panel (n°1, 2 et 5) ont mis en place un « compte erreur » dévolu à l'enregistrement de ce type de perte. S'agissant de la SGP n°3, l'impact financier lié à un incident opérationnel (s'il est supérieur au seuil de matérialité procédural) est pris en charge soit (option n°1) par la SGP elle-même (via ses propres ressources financières), soit (option n°2) par prélèvement sur la provision pour frais de gestion du fonds concerné. La SGP n°4, spécialisée dans le capital-investissement, n'applique que l'option n°1.

Les trois SGP ayant mis en place le « compte erreur » ont également mis en œuvre un exercice périodique de rapprochement comptable entre les mouvements constatés sur ce compte et le contenu du registre des incidents opérationnels. Cet exercice s'avère cependant insuffisant pour les SGP n°1 et 5 puisque la mission de contrôle a identifié une (faible) proportion d'incidents ayant eu un impact financier qui n'a pas été porté au « compte erreur ».

- Encadrement des risques opérationnels liés à l'externalisation ou à la délégation

Les cinq SGP du panel ont formalisé une cartographie de leurs prestataires (et délégataires) importants ou sensibles. La mission de contrôle en a sélectionné un échantillon (compris entre 5 et 6 acteurs par SGP) afin d'analyser les mesures prises pour éviter une aggravation indue du risque opérationnel dans le cadre de l'externalisation ou de la délégation. A titre d'exemple, l'échantillon retenu couvre des prestations d'agent comptable, de production de rapports de risques, de services informatiques, de fourniture de données ESG ou de suivi des portefeuilles.

La mission de contrôle a relevé qu'aucune des cinq SGP du panel n'avait intégré, à la phase de sélection des prestataires externes testés, la capacité de ces derniers à gérer efficacement les risques opérationnels associés aux services rendus.

Cette capacité est abordée formellement en revanche dans les contrats signés par les SGP n°2 et 4. Elle ne l'est que partiellement dans les contrats examinés signés par les SGP n°1 et 3. Elle n'est pas du tout abordée dans les contrats consultés signés par la SGP n°5.

S'agissant enfin du contrôle de la qualité des services rendus, il ne prend formellement en compte les incidents opérationnels rencontrés qu'au sein des SGP n°1 et 2.

➢ Lien entre le dispositif de traitement des réclamations et la gestion des risques opérationnels

Toutes les SGP contrôlées disposent d'un registre des réclamations. Les SGP n°2 à 5 n'y ont enregistré aucune réclamation sur la période sous contrôle.

Concernant la SGP n°1, en l'absence d'un identifiant commun utilisé à la fois dans le registre des réclamations et dans celui des incidents, il n'a pas été possible à la mission de contrôle de vérifier les liens éventuels entre des réclamations reçues et des incidents opérationnels subis. D'ailleurs, les fiches d'instruction des incidents opérationnels utilisées par cette SGP n'incluent pas de champ permettant de faire référence à une éventuelle réclamation associée.

Rappels réglementaires en lien avec les manquements constatés lors des contrôles :

Concernant l'enregistrement des incidents opérationnels :

- **Article 321-23 (VI), (VII) du RG AMF (OPCVM)** : « *[La SGP] […] VI. – […] établit et maintient opérationnel un système efficace de remontées hiérarchiques et de communication des informations à tous les niveaux pertinents. VII. – […] enregistre de manière adéquate et ordonnée le détail de ses activités et de son organisation interne.* » **(et articles 57 (1) (d), (e) du RD AIFM (FIA), 21 (1) (e) (f) du RD MIF II (GSM)) ;**
- **Article 321-81 (I) (a) du RG AMF (OPCVM) :** « *I. - La société de gestion de portefeuille adopte des dispositions, des procédures et des techniques appropriées et efficaces en vue : a) de mesurer et de gérer à tout moment les risques auxquels les OPCVM qu'elle gère sont exposés ou sont susceptibles d'être exposés, b) de garantir que les limites applicables aux OPCVM en matière de risque global et de contrepartie sont respectées, conformément aux articles 411-72 et 411-73 et aux articles 411-82 à 411-83.* » **(et article 39 (1) (a) (b) du RD AIFM, 23 (1) (a) (b) du RD MIF II) ;**
- **Article 13 (2) du RD AIFM :** « *2. Un gestionnaire établit une base de données historique, dans laquelle sont enregistrés tous les dysfonctionnements opérationnels, les pertes et les dommages. Cette base de données enregistre, de façon non limitative, les risques en matière de responsabilité professionnelle […] qui se sont concrétisés* ».

Concernant la comptabilisation des incidents :

- **Article 321-26 du RG AMF (OPCVM)** *: « La société de gestion de portefeuille établit et maintient opérationnelles des politiques et procédures comptables qui lui permettent de fournir en temps utile, à la requête de l'AMF, des informations financières qui offrent une image fidèle et sincère de sa situation financière et qui sont conformes à toutes les normes et règles comptables en vigueur ».* **(et articles 57 (4) du RD AIFM (FIA) et 21 (4) du RD MIF II (GSM)).**

Concernant les mesures prises en compte pour éviter une aggravation indue du risque opérationnel dans le cadre de l'externalisation ou de la délégation :

- **Article 321-96 (I), (II) (1), (2), (3), (5), (6), (10), (III) du RG AMF (OPCVM)** *: « I. - La société de gestion de portefeuille qui externalise une tâche ou fonction opérationnelle demeure pleinement responsable du respect de toutes ses obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier et se conforme en particulier aux conditions suivantes : (1)l'externalisation n'entraîne aucune délégation de la responsabilité des dirigeants ; (2) l'externalisation ne modifie ni les relations de la société de gestion de portefeuille avec ses clients ni ses obligations envers ceux-ci ; (3) l'externalisation n'altère pas les conditions ou les engagements auxquels était subordonné son agrément. (II) - La société de gestion de portefeuille agit avec toute la compétence, le soin et la diligence requis lorsqu'elle conclut, applique ou met fin à un contrat d'externalisation d'une tâche ou fonction opérationnelle essentielle ou importante. La société de gestion de portefeuille est en particulier tenue de prendre toutes les mesures pour que les conditions suivantes soient remplies : (1) le prestataire de services dispose des capacités, de la qualité et des éventuelles habilitations requises pour exécuter les tâches ou fonctions externalisées de manière fiable et*

professionnelle ; (2) le prestataire de services fournit les services externalisés de manière efficace. A cet effet, la société de gestion de portefeuille définit des méthodes d'évaluation du niveau de performance du prestataire de services ; (3) le prestataire de services surveille de manière appropriée l'exécution des tâches ou fonctions externalisées et gère de manière adéquate les risques découlant de l'externalisation ; (5) la société de gestion de portefeuille conserve l'expertise nécessaire pour contrôler effectivement les tâches ou fonctions externalisées et gère les risques découlant de l'externalisation, et procède au contrôle de ces tâches et à la gestion de ces risques. Pour l'application de cette disposition, la société de gestion de portefeuille conserve les ressources et l'expertise nécessaires à l'intégration effective des risques en matière de durabilité ; (6) le prestataire de services informe la société de gestion de portefeuille de tout événement susceptible d'avoir un impact sensible sur sa capacité à exécuter les tâches ou fonctions externalisées de manière efficace et conforme aux obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier qui leur sont applicables ; (10) le prestataire de services assure la protection des informations confidentielles ayant trait à la société de gestion de portefeuille ou à ses clients ; (III) - Les droits et obligations respectifs de la société de gestion de portefeuille et du prestataire de services sont clairement définis dans un contrat. » **(et articles 318-61 (I), (II) (1), (2), (3), (6), (10), (III) du RG AMF (FIA), 31 (1) (2) (a) (b) (c) (f) (j), (3) du RD MIF II (GSM)).**

Bonnes pratiques :

- Prévoir dans le registre des incidents opérationnels une typologie permettant d'identifier les incidents d'origine cyber[18], une évaluation du niveau de gravité des évènements identifiés ainsi qu'un champ dédié à l'entité (interne ou externe) ayant identifié le problème.
- Mettre en place une analyse consolidée *a posteriori* des causes des incidents opérationnels subis aux fins d'identification des causes des évènement récurrents et de pilotage des services rendus par les prestataires externes.
- Formaliser l'instruction des incidents opérationnels dans des fiches structurées, datées et signées, présentant l'événement survenu, évaluant sa gravité, ses causes probables et proposant des actions de remédiation en regard.
- Effectuer régulièrement un rapprochement entre les impacts financiers des incidents opérationnels enregistrés en comptabilité et les montants déclarés dans le registre des incidents.

Mauvaises pratiques :

- Omettre d'expliciter dans le registre des incidents les changements de méthode d'évaluation des impacts pouvant survenir d'un exercice à l'autre.
- Dissocier le suivi des incidents opérationnels et des plans de remédiation associés.
- Ne pas disposer d'un suivi des incidents d'origine informatique et cyber impactant les processus métier au motif que le système d'information utilisé est maintenu par un tiers.
- Multiplier les bases de suivi des incidents opérationnels sans veiller à leur réconciliation régulière ni à la cohérence de leur mode de renseignement.
- Ne pas prendre en compte les risques opérationnels associés aux services dont l'externalisation ou la délégation est souhaitée dès la phase de sélection des prestataires (ou délégataires) externes importants ou sensibles.
- Ne pas prévoir la réalisation d'analyses croisées des réclamations reçues et des incidents opérationnels subis afin de faciliter l'identification de causes partagées.

[18] Bonne pratique déjà identifiée pour partie dans la synthèse des contrôles SPOT « cybersécurité » n°2 publiée le 7 avril 2021 sur le site internet de l'AMF sous la forme suivante : « *Mettre en place et maintenir à jour une base des incidents d'origine cyber ou, a minima, identifier de manière univoque ces incidents lors de leur collecte dans la base des incidents opérationnels* » (https://www.amf-france.org/fr/actualites-publications/publications/syntheses-des-controles-spot/synthese-des-controles-spot-sur-le-dispositif-de-cyber-securite-des-societes-de-gestion-de).

3.4. MODALITES DE COUVERTURE DES RISQUES EN MATIERE DE RESPONSABILITE PROFESSIONNELLE

La majorité des SGP du panel disposent d'une double couverture contre les risques opérationnels associant la constitution d'un coussin de fonds propres supplémentaires à la souscription d'une assurance RCP. Néanmoins, les justifications du calcul ayant conduit à l'élaboration de ce coussin demeurent insuffisamment formalisées.

- Couverture des risques opérationnels via des fonds propres supplémentaires

Toutes les SGP du panel se sont dotées d'un coussin de fonds propres supplémentaires, y compris la SGP n°5 qui ne gère pas de FIA (en dépit de son agrément AIFM intégral). Cette SGP dispose dans ce cadre d'une poche de fonds propres supplémentaires de 15 k€.

Les quatre autres SGP du panel calculent ce coussin en utilisant la formule : « *Fonds propres supplémentaires : 0,01% x [Valeur absolue des FIA gérés]* ». Toutefois, aucune de ces quatre SGP n'a été en mesure de fournir les éléments justifiant du choix de ce taux de 0,01%, alors qu'il s'agit (règlementairement) d'un minimum. La SGP n°1 a expliqué, à l'issue des investigations, que la formule de calcul *supra* n'était retenue qu'à la condition de conduire à un montant supérieur au cumul des trois dernières années d'indemnisations versées (le montant cumulé sur trois ans des indemnisations versées s'appliquant dans le cas contraire).

- Couverture complémentaire via une assurance

Quatre SGP du panel (n°1, 3, 4 et 5) ont souscrit, en complément de la constitution d'un coussin de fonds propres supplémentaires, une assurance RCP couvrant les conséquences pécuniaires des incidents opérationnels subis ainsi que les frais de défense associés (en lien par exemple avec les plaintes introduites par des tiers). La SGP n°2 n'a pas souscrit d'assurance de ce type, s'appuyant sur le coussin cité pour se couvrir au regard des risques opérationnels liés à son activité.

En outre, les SGP n°1 à 4 ont également souscrit une assurance contre les risques d'origine cyber.

Aucun de ces deux types d'assurance n'a été activé au cours de la période sous contrôle.

SGP	n°1	n°2	n°3	n°4	n°5
Assurance RCP					
Niveau de couverture du contrat (M€)	90	N/A	30	50	2,5
Franchise du contrat (par sinistre, en M€)	40	N/A	0,25	0,1	Non communiquée
Assurance contre les risques d'origine cyber					
Niveau de couverture du contrat (M€)	235	35	15	5	N/A
Franchise du contrat (par sinistre, en M€)	40	1	0,1	0,07	N/A

Rappels réglementaires en lien avec les manquements constatés lors des contrôles :

Concernant les fonds propres supplémentaires dédiés à la couverture des risques en matière de responsabilité professionnelle :

- **Article 13 (3) du RD AIFM (FIA) :** « *3. Dans le cadre de la gestion des risques, le gestionnaire a recours à sa base de données historique interne et, le cas échéant, à des données externes, des analyses de scénarios et des facteurs reflétant l'environnement des affaires, ainsi qu'à des systèmes de contrôle interne.* » ;
- **Article 14 du RD AIFM (FIA)** : « *1. Les dispositions du présent article s'appliquent aux gestionnaires qui choisissent de couvrir leurs risques en matière de responsabilité professionnelle par des fonds propres supplémentaires. 2. Afin de couvrir les risques en matière de responsabilité pour négligence professionnelle, le gestionnaire fournit des fonds propres supplémentaires s'élevant au moins à 0,01 % de la valeur des*

portefeuilles des FIA gérés. La valeur des portefeuilles des FIA gérés correspond à la somme de la valeur absolue de tous les actifs détenus par tous les FIA gérés par le gestionnaire, y compris les actifs acquis grâce à l'effet de levier, les instruments dérivés étant alors évalués à leur valeur de marché. 3. L'exigence de fonds propres supplémentaires définie au paragraphe 2 est recalculée à la fin de chaque exercice et le montant de fonds propres supplémentaires est ajusté en conséquence. Le gestionnaire établit, met en œuvre et applique des procédures afin de suivre en permanence la valeur des portefeuilles des FIA gérés, calculée conformément au second alinéa du paragraphe 2. Si avant le recalcul annuel mentionné au premier alinéa, la valeur des portefeuilles des FIA gérés augmente sensiblement, le gestionnaire recalcule dans les meilleurs délais l'exigence de fonds propres supplémentaires et ajuste en conséquence le montant de ces derniers. […] » ;

- **Position-recommandation AMF DOC-2012-19, section 6.2.1, page 57** : citée *supra.*

Au regard de ces éléments règlementaires et de doctrine, l'AMF s'attendait à observer la **bonne pratique** consistant :

- à fonder le calcul des fonds propres supplémentaires sur une analyse prenant en compte à la fois le montant de ces fonds propres retenu au cours de l'exercice écoulé, les pertes opérationnelles liées aux incidents subis, les pertes potentielles liées aux incidents évités (*near miss*) et les résultats des travaux menés par le contrôle interne sur le dispositif de gestion des risques.

3.5. DISPOSITIF DE REPORTING RELATIF AUX INCIDENTS OPERATIONNELS SUBIS

Les SGP du panel ont mis en œuvre un *reporting* formel relatif au volume et aux impacts des incidents opérationnels subis à l'attention de leurs dirigeants responsables et – pour les trois SGP concernées – de leur maison-mère. Néanmoins, les règles conduisant à exclure certains incidents de ces *reportings* (pour des raisons de non-significativité par exemple) n'ont pas été formalisées par l'une des SGP du panel.

S'agissant des informations adressées à l'AMF via les FRA-RAC au regard du dispositif de gestion des risques opérationnels, elles se sont avérées significativement inexactes pour la plus importante SGP du panel (n°1) au regard du montant des pertes déclarées, en lien avec un défaut de méthode. Comme rappelé le 24 octobre 2023[19], à l'occasion de la publication de la synthèse SPOT sur les processus de production, de contrôle et de transmission à l'AMF des reportings réglementaires (dont la FRA-RAC) : « *[u]n tel niveau d'erreur n'est pas compatible avec l'importance cruciale des données transmises à l'Autorité dans le cadre de sa mission de supervision. Il plaide pour un renforcement important et rapide du dispositif de contrôle en place sur les processus de production de ces reportings* ».

3.5.1. A l'attention des dirigeants responsables

Le *reporting* adressé aux dirigeants est jugé qualitatif, sur l'ensemble de la période contrôlée, pour trois SGP sur cinq (n°1, 2 et 3). Il prend la forme de tableaux de bord au sein de la SGP n°1, complétés par un focus dédié aux incidents opérationnels dans le rapport annuel de conformité et de contrôle interne (cette dernière pratique ayant également été adoptée par la SGP n°5).

Au sein des SGP n°2 et 3 (qui présente un volume limité d'incidents sur la période analysée), ce *reporting* est exhaustif et effectué au fil de l'eau.

[19] https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/reportings-reglementaires-des-societes-de-gestion-lamf-appelle-une-plus-grande-rigueur

L'exhaustivité et la précision du reporting effectué sont discutables au sein des SGP n°4 et 5. En effet, celui de la SGP n°4 pâtit de la fragmentation des registres des incidents constatée *supra*[20]. S'agissant de la SGP n°5, la mission a relevé que les indemnisations versées au regard des pénalités CSDR[21] au cours de la période sous contrôle n'avaient pas été signalées aux dirigeants. Interrogée sur ce constat, la SGP l'avait justifié au regard du caractère jugé non significatif des montants en jeu[22]. Or, cette règle d'exclusion ne figure pas dans son corps procédural.

En revanche, les cinq SGP du panel ont prévu un processus accéléré de *reporting* aux dirigeants responsables des incidents opérationnels évalués comme particulièrement graves. Ce reporting exceptionnel est :

- Structurel, au sein des SGP n°2 et 5, dans la mesure où le dirigeant responsable est directement impliqué dans la chaîne de traitement de l'ensemble des incidents opérationnels subis ;
- Oral, au sein des SGP n°3 et 4, du fait de la proximité physique directe entre le RCCI et le dirigeant-responsable ;
- Adossé à l'appétit pour le risque opérationnel validé annuellement par la gouvernance de la SGP n°1 (le dépassement de cet appétit, par un incident unique ou plusieurs incidents cumulés, conduisant à l'information immédiate des dirigeants responsables).

3.5.2. A l'attention du groupe d'appartenance

Parmi les trois SGP appartenant à un groupe, deux (SGP n°1 et 2) ont mis en œuvre un *reporting* formel des incidents opérationnels significatifs vers leur maison-mère. En revanche, ce *reporting* n'est pas formalisé pour la SGP n°3**.**

3.5.3. A l'attention de l'AMF

La mission de contrôle a analysé les informations communiquées par les 5 SGP du panel à l'AMF relativement à leur dispositif de gestion des risques opérationnels dans les FRA-RAC émises sur la période sous revue.

Dans ces FRA-RAC, la SGP signale les principaux incidents enregistrés ainsi que les métriques suivies en termes de gestion des risques opérationnels. Parmi ces dernières, figurent (liste non limitative) :

- le nombre d'incidents classés par sévérité et par typologie ;
- le nombre d'anomalies constatées pour les prestataires de service critique ;
- le nombre de plan d'actions en retard ;
- le nombre de défaillances identifiées des systèmes informatiques ;
- le nombre de dépassements actifs des ratios d'investissements ;
- le nombre de VL qui ont fait l'objet d'un nouveau calcul après publication ;
- le nombre de procédures non mises à jour.

Les SGP évaluent également dans ces FRA-RAC le niveau de risque opérationnel associé à l'activité de gestion. Ce niveau est évalué comme « faible » par trois SGP sur cinq (n°1, 2 et 3) ou « moyen » pour les SGP n°4 et 5. Cette évaluation est justifiée, selon les SGP, par différents critères tels que les impacts financiers observés au cours de l'exercice écoulé, le corps procédural ainsi que le dispositif de contrôle interne en place.

---

[20] Cf. section 3.3.1.

[21] Montants facturés par le dépositaire ou le teneur de compte conservateur en application du règlement (UE) n°909/2014 (*Central Securities Depositories Regulation* ou « CSDR ») et de son règlement délégué (UE) 2017/389. Ces pénalités visent à sanctionner les retards de règlement-livraison d'instruments financiers, qu'ils résultent d'un défaut de livraison ou d'un retard de réception, imputables à la SGP.

[22] De l'ordre de quelques euros.

Enfin, chaque SGP du panel a déclaré dans les FRA-RAC consultées être en capacité d'évaluer le montant des pertes opérationnelles sur l'année écoulée. Le montant déclaré par ailleurs est en ligne avec celui évalué par la mission de contrôle à la lecture des registres des incidents pour trois SGP sur cinq (n°2, 3 et 4). En revanche, des écarts sont constatés pour les SGP n°1 et 5.

S'agissant de la SGP n°5, le montant de perte déclaré à l'AMF est supérieur à celui constaté dans le registre pour l'exercice 2022 (de l'ordre de quelques centaines d'euros). Il est en revanche inférieur de 7,2 k€ à celui constaté pour l'exercice 2024 (soit 68 % des pertes subies en lien avec des incidents opérationnels sur l'exercice).

S'agissant de la SGP n°1, le montant des pertes liées à des incidents opérationnels déclaré dans la FRA-RAC est surévalué par rapport à celui calculé à partir du registre, à hauteur de 4,4 M€ pour l'exercice 2022 et de 5,2 M€ pour l'exercice 2023. Ce montant des pertes déclaré à l'AMF est en revanche sous-évalué de 0,5 M€ pour l'exercice 2024. La SGP a expliqué que le montant intégré dans les FRA RAC correspondait à une estimation annuelle *a priori* du « coût du risque », certes validée par les instances internes, mais quasi-systématiquement différente des pertes effectivement constatées *a posteriori* au regard des incidents subis[23]. Or, c'est bien ce deuxième poste que vise la question « T2-B-2.1 » (« *quel est le montant ?* ») de la FRA-RAC en référence à la question précédente « T2-B-2 » (« *La société de gestion est-elle capable d'évaluer le montant des pertes opérationnelles sur l'année écoulée ?* »). **Ainsi, l'approche constatée, en faussant significativement le niveau de perte réel subi, est susceptible d'obérer la capacité de supervision de l'AMF sur le niveau de risque opérationnel porté dans la durée par cet acteur.**

Rappels réglementaires en lien avec les manquements constatés lors des contrôles :

Concernant le *reporting* aux instances dirigeantes et à l'AMF relativement aux incidents opérationnels :

- **Article 321-23 (VI), (VII) du RG AMF (OPCVM)** : cité *supra* **(et articles 57 (1) (d), (e) du RD AIFM (FIA), 21 (1) (e) (f) du RD MIF II (GSM)) ;**
- **Article 321-75-1 du RG AMF (OPCVM) :** « *En application de l'article L. 621-8-4 du code monétaire et financier, la société de gestion de portefeuille communique à l'AMF au plus tard un mois calendaire suivant la fin de chaque trimestre de l'année civile : (1) Une information relative aux indemnisations versées par la société de gestion de portefeuille aux actionnaires ou porteurs de parts des OPCVM qu'elle gère, y compris par délégation et aux clients à qui la société de gestion de portefeuille fournit un ou plusieurs services d'investissement ou services connexes. Lorsque la société de gestion de portefeuille n'a pas versé d'indemnisation au cours de la période couverte, elle en informe également l'AMF ; (2) Une information relative au non-respect par la société de gestion de portefeuille des règles d'investissement et de composition de l'actif prévues par les dispositions législatives ou réglementaires et les documents destinés à l'information des investisseurs des OPCVM qu'elle gère, y compris par délégation, à l'exception des cas de non-respect de ces règles intervenant indépendamment de la volonté de la société de gestion de portefeuille et ne résultant pas de l'arrivée à échéance d'un instrument financier détenu par l'OPCVM. Le présent article n'est pas applicable aux sociétés de gestion de portefeuille gérant par délégation un OPCVM lorsque la société de gestion dudit OPCVM est déjà soumise aux obligations de communication requises en application du présent article.* » **(et article 318-37-1 du RG AMF (FIA)).**

Bonnes pratiques :

- Prévoir un processus accéléré de *reporting* aux dirigeants responsables des incidents opérationnels évalués comme particulièrement graves.
- Inclure, dans le rapport annuel de conformité et de contrôle interne, un focus sur les principaux incidents opérationnels identifiés au cours de l'exercice écoulé, ainsi que sur l'état d'avancement des plans de remédiation convenus au regard des incidents dont l'impact a dépassé le seuil de matérialité convenu.

[23] En l'occurrence le comité des risques opérationnels et le comité des risques du groupe (cf. section 3.1.3 *supra*).

Mauvaises pratiques :

- Omettre de formaliser dans le corps procédural les seuils de matérialité en-deçà desquels les incidents opérationnels subis ne sont pas rapportés aux dirigeants responsables.
- Réduire le *reporting* relatif aux incidents opérationnels significatifs adressé au groupe à de simples échanges informels.

3.6. DISPOSITIF DE CONTROLE INTERNE APPLIQUE A LA GESTION DES RISQUES OPERATIONNELS

Pour les cinq SGP du panel, le dispositif de contrôle relatif à la gestion des risques opérationnels est supervisé par des comités internes compétents en matière de contrôle interne, de conformité ou de gestion des risques. S'agissant du contrôle périodique, celui-ci est soit pris en charge par le groupe soit délégué à des prestataires externes[24].

Les travaux menés par le contrôle interne ont permis à la SGP n°1 d'engager un chantier de remédiation des processus de travail du *middle office* en lien avec la récurrence constatée des incidents opérationnels impactant ce périmètre. En revanche, la SGP n°4 n'a pas mis en œuvre de rapport d'instruction formalisé des incidents opérationnels subis malgré une recommandation en ce sens de sa fonction de contrôle permanent en 2023.

3.6.1. Travaux réalisés par le contrôle permanent

La fonction de contrôle permanent est assurée par une équipe interne dans les cinq SGP du panel, sans délégation à un prestataire externe. Le RCCI de chacune de ces SGP rapporte à un dirigeant responsable.

Le dispositif de gestion des risques opérationnels a fait l'objet d'au moins une mission du contrôle permanent au cours des trois exercices contrôlés. En fonction des SGP, ces travaux ont porté sur la qualité de l'instruction des incidents, le calcul du coussin de fonds propres supplémentaires ou le suivi des prestations externalisées.

Dans ce cadre, en lien avec la recrudescence constatée au T1 2023 des incidents opérationnels impactant le *middle office*, la SGP n°1 a décidé le lancement d'une *task force* dédiée à l'amélioration des processus concernés, en y associant la gestion, l'informatique et les fonctions en charge de la gestion des risques.

Les recommandations formulées à l'issue des travaux de contrôle permanent menés ont fait l'objet d'un suivi satisfaisant, sauf au sein des SGP n°2 et 4. En effet, s'agissant de la SGP n°2, l'absence de test complet du PCA, constaté par la mission de contrôle[25], avait fait l'objet de trois recommandations successives émises, au cours de la période sous revue, à l'attention des dirigeants responsables. Ces recommandations avaient été émises par la RCCI (en novembre 2022 puis en décembre 2023), ainsi que, en décembre 2024, par la fonction de contrôle permanent du groupe. Quant à la SGP n°4, bien que les travaux du contrôle permanent aient conduit à recommander, en 2023, de « *collecter systématiquement les rapports d'incidents et de les enregistrer dans la base de données* », la formalisation systématique des fiches incidents n'était toujours pas en place à date de contrôle par l'AMF.

3.6.2. Travaux réalisés par le contrôle périodique

La fonction de contrôle périodique est assurée par une équipe du groupe dans les SGP n°1, 2 et 3. Elle est déléguée à un prestataire externe par les SGP indépendantes du panel (n°4 et 5).

---

[24] A raison de 6 jours hommes par an pour la SGP n°2, 24 jours hommes par an pour la SGP n°4 et 5 jours hommes par an pour la SGP n°5.

[25] Cf. section 3.2.4 *supra*.

A l'instar de ce qui est constaté *supra*, pour les cinq SGP du panel, le dispositif de gestion des risques opérationnels a fait l'objet d'au moins une mission de contrôle périodique durant la période contrôlée. Ce thème a été soit ciblé directement par une telle mission (c'est le cas par exemple pour les SGP n°4 et 5), soit inclus dans les travaux menés sur une thématique plus large (par exemple pour la SGP n°1 qui a procédé de la sorte dans le cadre des audits menés sur le *middle office* ou la production informatique).

Les recommandations émises à l'issue de ces audits ont fait l'objet d'un traitement satisfaisant, sauf pour la SGP n°3 qui a clôturé sans suite la préconisation visant au partage d'information avec le groupe concernant les incidents d'origine cyber rencontrés par l'infrastructure informatique partagée.

Enfin, les travaux menés par le contrôle interne sont partagés avec les dirigeants responsables dans le cadre d'un comité dédié par l'ensemble des SGP du panel.

Rappels réglementaires en lien avec les manquements constatés lors des contrôles :

- **Article 321-23 (IV) du RG AMF (OPCVM)** : « *[La SGP] établit, met en œuvre et maintient opérationnels des mécanismes de contrôle interne appropriés, conçus pour garantir le respect des décisions et des procédures à tous les niveaux de la SGP* » **(et articles 57 (1) (c) du RD AIFM (FIA), 21 (1) (c) du RD MIF II (GSM)) ;**
- **Article 321-27 du RG AMF (OPCVM)** : « *6. Le gestionnaire contrôle et évalue régulièrement l'adéquation et l'efficacité des systèmes, mécanismes de contrôle interne et autres dispositifs mis en place en application des paragraphes 1 à 5, et prend des mesures appropriées pour remédier à d'éventuelles défaillances.* » **(et articles 57 (6) du RD AIFM (FIA), 21 (5) du RD MIF II (GSM)) ;**
- **Article 321-31 (I) (1) du RG AMF (OPCVM)** : « *2. Le gestionnaire établit et maintient opérationnelle une fonction permanente et efficace de vérification de la conformité, qui fonctionne de manière indépendante et assume les responsabilités suivantes: a) contrôler et, à intervalles réguliers, évaluer l'adéquation et l'efficacité des mesures, politiques et procédures mises en place en application du paragraphe 1, ainsi que des actions entreprises pour remédier à d'éventuels manquements du gestionnaire à ses obligations* » **(et article 61 (2) (a) du RD AIFM (FIA), 22 (2) (a) du RD MIF II (GSM)).**

Bonne pratique :

- Mettre en place des groupes de travail trans-directions en charge d'identifier et de remédier aux causes des incidents opérationnels récurrents.