

Atelier FRA/RAC 2025

Webinaire du 6 mars 2025



I – FRA/RAC





**Activités accessoires
(au sens de la section 2.B
« Activité accessoires » de
l’instruction AMF DOC-2008-03 »**



T1-B-7

- **Nouveau :**

« Mandats d'arbitrage en unité de compte (y compris par délégation) »

- **Avant :**

« Mandats d'arbitrage dans le cadre de contrats d'assurance vie libellé en unités de compte »



Clientèle – assiette de calcul du mécanisme de garantie des services des sociétés de gestion

(articles L312-4-1, L322-5 et L322-9 du Code
Monétaire et Financier)



T1-D-1

« La SGP gère-t-elle des fonds dont tout ou partie du passif est tenu sous forme nominative ? » (Oui/Non)

- *Les points suivants : T1-D-2 à T1-D-5 doivent être complété uniquement si la réponse indiquée est « Oui » pour T1-D-1.*
- *Si la SGP n'est pas concerné par le 1^{er} point, les autres points sont non-applicable à la SGP.*

T1-D-3

« Valeur des actifs gérés sous mandat pour la clientèle couverte par le fonds de garantie des dépôts et de résolution » (**Nombre en K€**)

Question :

-Est-ce que ça couvre uniquement la trésorerie du fonds couvert par la banque dépositaire adhérente au FGDR ?

-Est-ce que ça couvre les encours des clients non professionnels ? Ou personnes physiques ?

Réponse :

D'après les indications de l'arrêté du 5 août 2022 pris pour l'application du 1 de l'article L.322-9 du code monétaire et financier et relatif à la garantie des services des sociétés de gestion.

La question renvoie à la typologie de clientèle qui serait couverte en cas de sinistre (dans les cas prévus à l'arrêté du 5 août 2022), à savoir l'ensemble de la clientèle à l'exception des typologies de clients listés au II de l'article L.312-4-1 du code monétaire et financier et exclus de la couverture, en substance la clientèle « institutionnelle ».

Par conséquent, renseigner le montant des encours gérés sous mandat (hors clientèle institutionnelle).

Exemple : S'il s'agit d'un client institutionnel catégoriser en « non-professionnel » il est exclu au sens de l'article 312-4-1 du code monétaire et financier.



Commercialisation des placements
collectifs distribués par la société
de gestion
(en France et à l'étranger)



T1-J-14

- **Nouveau point cette année :**

« Nombre de documents commerciaux au format texte (PDF, Word, PowerPoint, ...) diffusés directement aux clients ou mis à disposition de conseillers en investissement à cette fin sur le périmètre des fonds accessibles à une clientèle non professionnelle (ne pas comptabiliser les fiches d'information ni les fiches techniques) »

- **Explication :**

Ce point fait référence à la position recommandation AMF DOC 2011-24, par documents commerciaux, il fait référence à toute information à caractère promotionnel adressée directement à des investisseurs potentiels ou existants ou susceptible d'être relayée par les distributeurs, à l'écrit, auprès de leurs clients potentiels ou existants.

Question :

Lorsqu'un support fait l'objet de plusieurs mises à jour (ajout de slides etc), pouvez-vous confirmer que nous devons le considérer comme 1 seul support à faire remonter ?

Réponse :

Cette question renvoie aux recommandations de l'AMF dans la DOC-2011-24 "Guide pour la rédaction des communications publicitaires et la commercialisation des placements collectifs et des SOFICA"

Page 3 de la DOC-2011-24 :

Aux fins du présent guide, par « communications publicitaires », on entend toute information à caractère promotionnel adressée directement à des investisseurs potentiels ou existants ou susceptible d'être relayée par les distributeurs, à l'écrit ou à l'oral, auprès de leurs clients potentiels ou existants.

Parmi les documents pouvant être considérés comme des communications publicitaires, aux fins du présent guide, on peut citer les exemples suivants :

--> Voir la liste dans le DOC-2011-24

On comprend donc que si le document a été transmis à des clients, et qu'on transmet le même document avec des m à j, ce document constitue un nouveau document donc doit être comptabilisé.



Dispositif de cyber sécurité – préparation à DORA



T1-0-1

« La SGP a-t-elle été victime d'une ou plusieurs attaques cyber au cours de l'exercice écoulé ? »

Question 1:

Dans le cas d'un groupe avec un partage des serveurs, il est difficile de faire remonter des attaques visant la SGP (et non le groupe ou d'autres activités) : devons-nous donc faire remonter le nombre d'incident au niveau groupe ?

Question 2 :

Faut-il lister les attaques réussies uniquement ou toutes les attaques ?

Réponse 2 :

Il faut lister toutes les attaques.

Distinction à faire entre "Attaque" et "Incident" :

Les attaques comprennent l'ensemble des tentatives abouties ou non.

Un incident est une attaque aboutie / réussie par l'assaillant.

Confirmer ce point avec l'AMF car une attaque aboutie correspond donc à un incident.

Point est à éclaircir avec l'AMF concernant les incidents du groupe duquel dépend la SGP.

T1-0-2

« Avez-vous effectué des déclarations d'attaques à l'AMF au cours de l'exercice écoulé ? »

Question :

Sauf erreur, sur l'exercice 2024, ces éléments n'étaient pas à déclarer à l'AMF, mais seulement à la BCE.

Réponse :

Il est par ailleurs rappelé que la SGP doit être organisée de manière à informer

« sans délai l'AMF des incidents dont la survenance est susceptible d'entraîner pour la SGP une perte ou un gain, un coût lié

- à la mise en cause de sa responsabilité civile ou pénale,
- à une sanction administrative
- ou à une atteinte à sa réputation
- et résultant du non-respect des [règles d'organisation générale]

d'un montant brut dépassant 5 % de ses fonds propres réglementaires. »

(articles 321-35 (SGP d'OPCVM ou de FIA sous les seuils de la directive AIFM et n'ayant pas opté pour l'application intégrale de celle-ci) et 318-6 (SGP de FIA soumises intégralement à la directive AIFM) du règlement général de l'AMF).

T1-0-3.1

« Quel a été le nombre d'incidents issus de ces attaques (attaques réussies se traduisant par des perturbations du système d'information, de la disponibilité des services, des pertes de données, ...) ? »

- **Indication complémentaire :**

Ce point ne parle pas des incidents en eux même, mais des « impacts » de ces incidents.

T1-O-3.3

« Quel a été le nombre d'incidents majeurs selon DORA ? »

Question :

DORA étant entré en vigueur en janvier 2025, qu'est-il attendu ? Une analyse a posteriori des incidents 2024 ? Si tel est le cas, cela est complexe à réaliser

Cette question s'affiche uniquement dans le cas :

Si "Oui" à la question T1-O-3, la question devient obligatoire et s'affiche.

T1-O-3 : La SGP a-t-elle été victime d'un ou plusieurs incidents cyber ayant eu un impact sur l'activité de la SGP au cours de l'exercice écoulé ?

Confirmer avec l'AMF sur ce point, dans le cas où il y a eu une cyber attaque ayant eu un impact sur l'activité de la SGP, qu'est-ce qui est attendu par l'AMF, faut-il réaliser des analyses de l'incident en question a posteriori ?

T1-O-10

« Quelles mesures du guide suivant de l'ANSSI en matière de sauvegarde de données n'implémentez-vous pas ? »

- **Précision :**

Ce point fait référence aux essentiels de l'ANSSI concernant les sauvegardes des systèmes d'information à savoir :

LES ESSENTIELS

SAUVEGARDE DES SYSTÈMES D'INFORMATION

1/ CONSTRUIRE ET PROTÉGER

- Définir une **politique de sauvegarde** en identifiant les données critiques pour l'activité de votre entité en précisant la fréquence à laquelle il est important de les sauvegarder.
- Considérer les opérations de sauvegarde et de restauration comme des **opérations sensibles d'administration** devant bénéficier des protections adéquates : poste d'administration durci, flux dans un réseau d'administration, etc.
- Rendre indépendante l'**infrastructure de sauvegarde** vis-à-vis des annuaires de production (ex. : Active Directory).
- S'assurer du **contrôle d'accès des sauvegardes** pour garantir qu'elles ne seront ni modifiées ni altérées et toujours disponibles, en particulier dans le cadre de l'utilisation d'offres de sauvegarde *cloud*.
- Être **vigilant sur la sensibilité des données sauvegardées** en cas de solution hors-site, dans un *cloud* public ou chez un prestataire externe. Chiffrer les sauvegardes au préalable par vos propres moyens si nécessaire.
- Faire évoluer continuellement l'**infrastructure de sauvegarde** au même rythme que l'évolution des SI (virtualisation, *cloud*, etc.) et en fonction de l'évolution de la menace. Ne conservez pas une infrastructure obsolète en production.

2/ ANTICIPER ET RÉAGIR

- Définir une **stratégie de restauration**, en lien avec le plan de reprise d'activité et en tenant compte des principaux scénarios d'attaque identifiés sur les SI (rançongiciels, espionnage, etc.). **Réaliser régulièrement des tests de restauration**. Impliquer la direction sur les modes dégradés acceptables en cas de crise cyber.
- **Ne pas oublier d'inclure les médias d'installation et les configurations** des applications métier dans les sauvegardes.
- **Réaliser régulièrement et impérativement des sauvegardes hors-ligne** (déconnectées du SI).
- **Prévoir une procédure d'isolation d'urgence** du système de sauvegarde (serveurs, médias, etc.) en cas de suspicion de compromission ou d'attaque en cours.
- Après un incident, tenir compte du fait que les sauvegardes peuvent contenir les vecteurs de compromission. **Restaurer à partir de sources de confiance** (images officielles, binaires d'installation signés), contrôler la conformité des configurations, faire un scan antivirus des données.

T1-O-11

« Quels sont les principaux composants humains, organisationnels et techniques constituant votre dispositif de détection d'évènements redoutés de cybersécurité ? »

- **Précision :**

Il convient de répondre à cette question de manière succincte, à savoir, quand une entreprise dispose d'un SOC : périmètre couvert, périmètre non couvert, indicateurs, et coût.

Un SOC (Security Operations Center) est mis en place via une équipe interne ou externalisée de professionnels de la sécurité informatique dédiée à la surveillance de l'ensemble de l'infrastructure informatique d'une organisation.

Un SOC offre une surveillance continue de vos systèmes informatiques. La détection instantanée des menaces en temps réel. L'analyse approfondie des risques. Et la réaction rapide face aux vulnérabilités détectées.



Conflits d'intérêts

(selon le cas art. 318-12 à 318-14 du RGAMF et articles 30 à 36 du règlement délégué (UE) 231/2013 de la Commission du 19 décembre 2012 et/ou 321-46 à 321-52 du RGAMF et/ou art. 33 et suivants du règlement délégué (UE) 2017/565 de la Commission du 25 avril 2016)



T2-E-8.1 et T2-E-8.2

T2-E-8.1

« Combien de participations non cotées font l'objet d'investissement directement ou indirectement sur le même émetteur (dette ou capital) par au moins deux fonds gérés par la SGP ? »

T2-E-8.2

« Combien de participations non cotées font l'objet d'investissement directement ou indirectement sur un même émetteur en dette d'une part et en capital d'autre part par des fonds différents gérés par la SGP ? »

Précision :

La mention « indirectement » dans les deux points fait référence aux fonds de fonds.

Question :

Quelle distinction entre **T2-E-8.1** et **T2-E-8.2** ?

Réponse :

On comprend que la question **T2-E-8.1** correspond à un co-invest de même nature et que **T2-E-8.2** correspond à un co-invest avec des instruments de nature différentes donc problème de conflit d'intérêts

T2-E-8.2

T2-E-8.2

« Combien de participations non cotées font l'objet d'investissement directement ou indirectement sur un même émetteur en dette d'une part et en capital d'autre part par des fonds différents gérés par la SGP ? »

Question :

S'agit-il du nombre d'opérations de ce type qui ont eu lieu au cours de l'exercice ou bien le nombre d'investissement dans cette position durant l'exercice (incluant des opérations de co-investissement ayant closé plusieurs années auparavant) ?

Réponse :

Au cours de l'exercice et n'incluant pas les opérations des exercices précédentes.



Tenue du passif



T2-V-1 à T2-V-1.7.3 (Supprimé)

- **Explication :**

Ces points seront inclus dans le cadre d'un questionnaire ROSA dédiée.



Gestion de portefeuille pour le compte de tiers (gestion sous mandat)



T2-W-11

T2-W-11

« Encours investis dans des parts de fonds intragroupe dont le niveau de frais est calibré pour permettre le paiement de rétrocessions lorsque le service effectué par le distributeur le permet (parts « retail ») – hors MMF et ETF »

T2-W-12

« Proportion des encours investis dans des parts de fonds intragroupe dont le niveau de frais est calibré pour permettre le paiement de rétrocessions lorsque le service effectué par le distributeur le permet (parts « retail ») – hors MMF et ETF

- **Précision :**

Parmi les classes de parts accessibles à la clientèle de détail les « parts retail », qui s'entendent par opposition aux « parts clean shares » dont les frais sont réduits (ne faisant pas l'objet de rétrocessions).



II – Rappel sur les fonds propres



Schéma 1 : Exigence quantitative

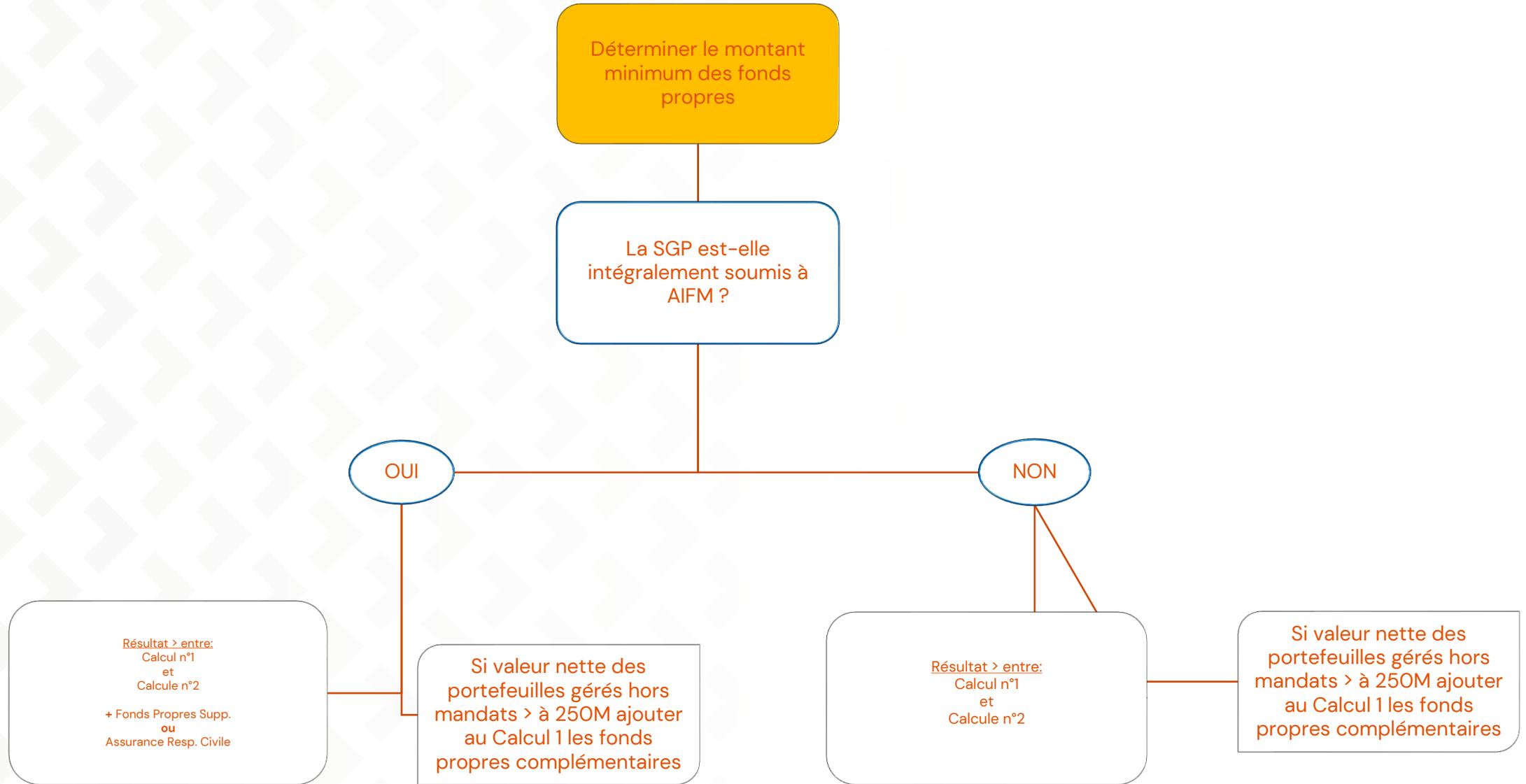


Schéma 2 : Exigence qualitative

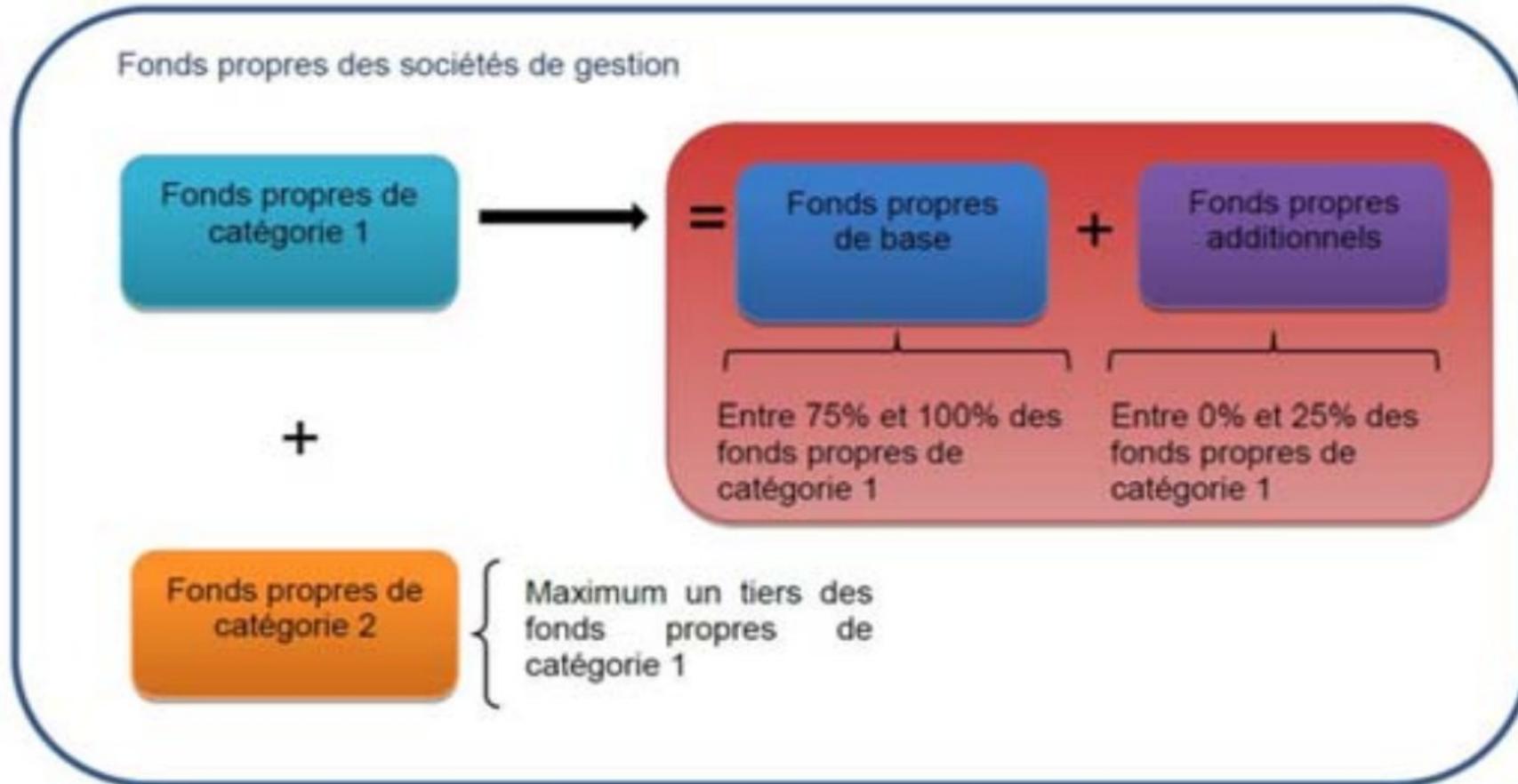
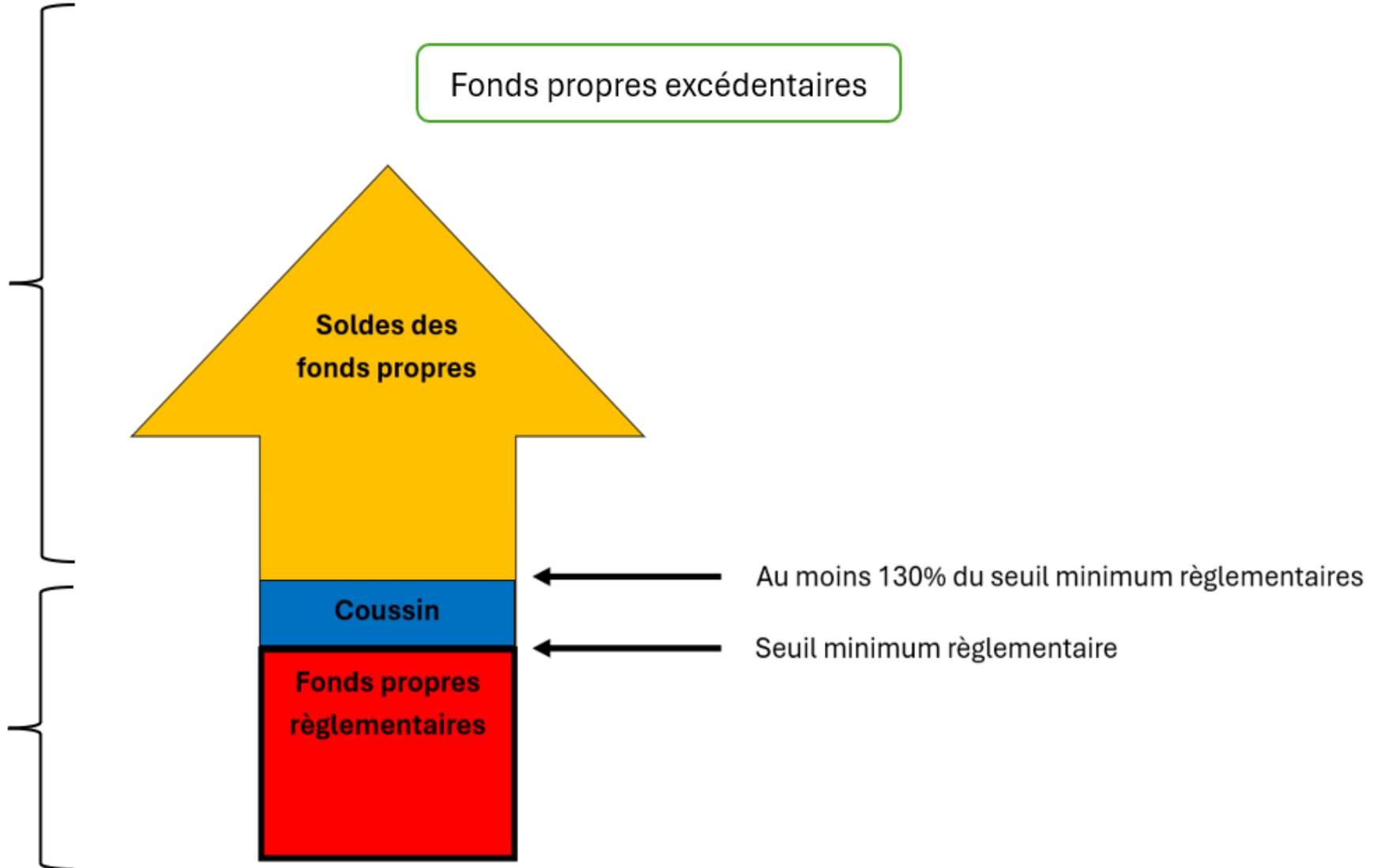


Schéma 3 : Exigence de placement

L'investissement dans des actifs « risqués » (moins liquides et/ou spéculatifs) est autorisé à la condition d'avoir préalablement constitué un « coussin » d'au moins 30 %.
(Articles 317-3 et 321-11 du RGAMF à condition de ne pas faire peser un risque substantiel sur le niveau de fonds propres)

Les fonds propres doivent être placés dans des actifs liquides et non spéculatifs.
(Articles 317-3 et 321-11 du RGAMF)





III – Priorités de supervision AMF pour 2025



Gestion d'actifs

- **Risques opérationnels**
→ Contrôle SPOT à venir en 2025.
- **Fonctions conformité et de contrôle interne**
→ Déjà un contrôle SPOT en 2020 mais un prochain va arriver en 2025.
- **Valorisation et transfert d'actifs entre portefeuille dans l'immobilier et le non-côté**
→ Des travaux spécifiques seront menés par l'AMF sur ces pratiques en 2025.

Commercialisation

- **Implication de la fonction de vérification de la conformité dans les processus transverses relatifs à la conduite des collaborateurs**
→ Nouvelle série de contrôle SPOT en 2025.
- **Communication clients concernant les produits peu liquides**
→ Contrôle SPOT à venir 2025.
- **Parcours digitalisés proposés aux clients non professionnels**
→ Contrôle SPOT à venir 2025.



IV – Rappel des
dernières
sanction/transaction
AMF



Transaction 2025

Les anomalies relevées sont les suivantes :

- Défaillances dans le dispositif de contrôle interne
- Insuffisances dans la documentation des décisions d'investissement
- Lacunes dans la gestion des conflits d'intérêts
- Manquements aux obligations de reporting réglementaire
- Insuffisances dans la documentation des procédures opérationnelles

Rendez-vous sur
www.franceinvest.eu

Et sur nos réseaux sociaux :

