AUTORITÉ DES MARCHÉS FINANCIERS

Impression à partir d'une page du site internet de l'AMF

21 décembre 2023

L'AMF publie la synthèse d'une troisième campagne de contrôles thématiques sur les dispositifs de cybersécurité des sociétés de gestion

Le risque cyber constitue l'un des principaux risques identifiés par l'AMF dans sa cartographie des risques. Dans la perspective de la mise en œuvre du règlement européen sur la résilience opérationnelle numérique (DORA) et en lien avec sa cartographie des risques, l'Autorité des marchés financiers a examiné les dispositifs de supervision des risques d'origine cyber de 5 établissements dans le cadre des relations entretenues avec leurs principaux prestataires informatiques et partenaires. Elle encourage les sociétés de gestion à renforcer ces dispositifs et à une approche plus proactive vis-à-vis de ce type de risque.

Après deux premiers exercices dont elle a publié les enseignements en 2019 et 2021, l'AMF a analysé, à l'occasion d'une nouvelle série de contrôles thématiques courts (SPOT), les pratiques de 5 nouvelles sociétés de gestion de taille moyenne pour faire face au risque cyber. Ce dernier est défini comme découlant d'une atteinte malveillante potentielle à la disponibilité, l'intégrité, la confidentialité des données ou à la traçabilité des actions au sein des systèmes d'information des établissements du panel. L'AMF a concentré son analyse sur les services rendus par les prestataires informatiques clés, notamment ceux fournissant un service informatique en nuage (*cloud*). Elle s'est également intéressée aux canaux informatiques d'échanges de données sensibles mis en place avec les autres partenaires des sociétés du panel, à savoir les dépositaires, les valorisateurs, les teneurs de comptes-conservateurs, les commissaires aux comptes, les apporteurs d'affaires et les distributeurs.

Les points d'attention de l'AMF ont porté sur :

- l'organisation et la gouvernance de la cybersécurité, ainsi que les procédures associées ;
- le processus de sélection et de contractualisation avec les prestataires informatiques et les partenaires ;
- le dispositif de contrôle de l'ensemble.

Dans son document de synthèse, l'AMF constate que la majorité des sociétés de gestion contrôlées ont formalisé une cartographie exhaustive de leurs prestataires informatiques sensibles, incluant une évaluation du niveau de risque pour chacun d'entre eux. Mais cet exercice de cartographie n'a pas été réalisé à l'identique sur le périmètre des autres partenaires. Dès lors, les sociétés de gestion n'ont pas mis en place tous les outils de supervision nécessaires pour s'assurer de l'usage systématique, par leurs collaborateurs, des canaux informatiques d'échanges appropriés en fonction du niveau de sensibilité des données échangées.

L'AMF constate par ailleurs une prise en compte insuffisante, lors de la phase de sélection et de contractualisation des prestataires informatiques et des autres partenaires, des critères relatifs à la robustesse des dispositifs de cybersécurité, de gestion des incidents et de continuité d'activité associés aux services rendus. Cependant, les sociétés de gestion du panel déploient des contrôles a posteriori ciblant l'efficacité de ces dispositifs. Ces contrôles prennent la forme de vérifications opérées par les utilisateurs et de contrôles permanents ou périodiques, ces derniers pouvant inclure des tests techniques.

Il ressort de cette nouvelle campagne de contrôles SPOT la persistance de plusieurs anomalies standards. Par ailleurs, les entités examinées ont adopté une approche davantage réactive que proactive s'agissant des risques d'origine cyber associés aux prestations externalisées, qui ne correspond pas à l'approche défendue par la règlementation européenne DORA (*Digital Operational Resilience Act*), qui s'appliquera à partir du le 17 janvier 2025, et qui inclut notamment des principes clés de gestion des risques liés aux prestataires informatiques. DORA propose en effet un équilibre entre les mesures réactives (mécanisme d'examen des incidents, stratégie de continuité des activités) et proactives (classification préalable des sources de risques d'origine cyber, élaboration d'une politique de sécurité de l'information).

Cette troisième série de contrôles marque la fin de la phase de pédagogie amorcée par l'AMF dès 2019 sur les risques d'origine cyber. Si elles devaient perdurer à l'avenir, les fragilités exposées dans cette synthèse et dans les deux précédentes pourraient justifier le déclenchement d'une action répressive.

À propos de l'AMF

Autorité publique indépendante, l'AMF est chargée de veiller à la protection de l'épargne investie en produits financiers, à l'information des investisseurs et au bon fonctionnement des marchés. Visitez notre site : https://www.amf-france.org URL = [https://www.amf-france.org]

CONTACT PRESSE

- Direction de la communication

+33 (0)1 53 45 60 25
media@amf-france.org

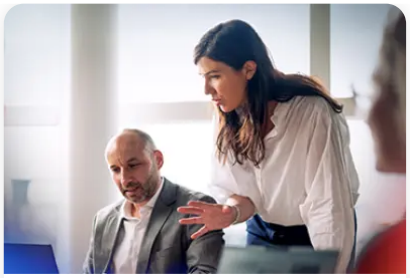
En savoir plus

- Synthèse des contrôles SPOT relative au dispositif de cybersécurité des sociétés de gestion de portefeuille N°3 - 2023

Mots clés GESTION D'ACTIFS

SUR LE MÊME THÈME

S'abonner à nos alertes et flux RSS

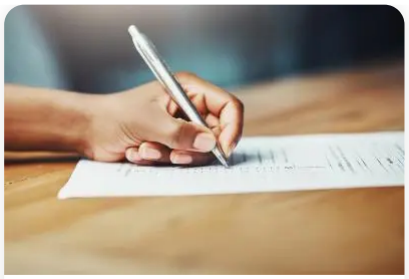


ACTUALITÉ

FONDS MONÉTAIRES

21 mai 2026

L’AMF se conforme aux orientations de l’ESMA sur la mise à jour des paramètres de scénarios de crise, prévue à l’article 28 du règlement sur les fonds monétaires, pour [illegible]26

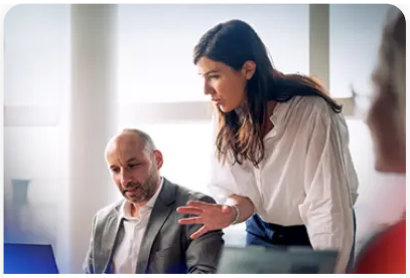


BLOG MÉDIATEUR

GESTION D'ACTIFS

18 mai 2026

Retrait de parts de SCPI : où placer dans le registre chronologique les demandes incomplètes ?



ACTUALITÉ

GESTION D'ACTIFS

13 mai 2026

Outil de gestion de la liquidité : l'AMF a l’intention d’appliquer les orientations de l'ESMA

Mentions légales :
Responsable de la publication : Le Directeur de la Direction de la communication de l'AMF. Contact : Direction de la communication, Autorité des marchés financiers - 17, place de la Bourse - 75082 Paris Cedex 02