ARCAD

NEWS – Part 2/3 bis: Précisions sur les organisations IT et sur la sous-traitance informatique des Gestionnaires de Fond d'Investissement (GFI)

Ce qu'il faut retenir !

10/01/2019

Introduction

La circulaire CSSF 18/698 apporte des précisions sur l'organisation informatique et sur la circulaire CSSF 17/654 relative à la sous-traitance informatique reposant sur une **infrastructure informatique en nuage** ou une **infrastructure de « Cloud Computing »**. Nous allons dans cette newsletter aborder les différents points à retenir y afférent.

Précision sur l'organisation informatique

Les principes généraux concernant l'infrastructure technique et informatique ont été modifiés par la circulaire CSSF 18/698 qui abroge la circulaire CSSF 12/546 telle que modifiée.

Chaque GFI doit se doter dans ses locaux d'une infrastructure technique et informatique adaptée à l'activité qu'il veut réaliser. En effet, le GFI doit établir, mettre en œuvre et garder opérationnels des systèmes et des procédures appropriés pour préserver la sécurité, l'intégrité et la confidentialité des informations, en tenant compte de la nature des informations concernées.

Ces exigences sont remplies au mieux lorsque le GFI dispose de sa propre infrastructure informatique. Celle-ci est prise en charge par le service informatique du GFI, qui est, à son tour, organisé et encadré par un dispositif de contrôle interne fixé par les instances dirigeantes.

Le GFI doit mettre en œuvre des procédures et un dispositif lui permettant d'identifier et de gérer les risques informatiques dans les domaines suivants :

- le risque d'atteinte à la confidentialité, à l'intégrité et à l'accessibilité des données ;
- les risques liés à la continuité des activités du GFI et à la capacité de résilience des systèmes informatiques ;
- les risques liés à l'externalisation de la fonction informatique, le cas échéant ;
- le risque de fraude informatique, caractérisé par l'usage de données, de logiciels et de matériel informatique du GFI à des fins malicieuses ;
- les risques de cyberattaques.

La CSSF rappelle que chaque GFI est tenu de respecter les dispositions de la circulaire CSSF 11/504 concernant les fraudes et incidents dus à des attaques informatiques externes.

En cas d'indisponibilité de son système informatique, le GFI doit être en mesure de fonctionner normalement. Il doit, pour se faire, prévoir une solution de « back-up » en adéquation avec le plan de continuité de ses activités. Le plan de continuité doit décrire les actions à implémenter afin de poursuivre les activités en cas d'incident ou de sinistre lié à des événements anormaux.

Sous-traitance informatique

Les dispositions citées préalablement n'empêchent toutefois pas un GFI de recourir, sous sa responsabilité, aux services d'un tiers spécialisé en matière de conseil, de programmation, de maintenance ou de gestion de systèmes informatiques.

Tout recours à un tiers doit être notifié préalablement à la CSSF et être formalisé par un contrat de services. Le tiers doit, en outre, faire l'objet d'une due diligence initiale et d'un suivi continu, en accord avec le sous-chapitre 6.2. « Encadrement de la délégation » de la circulaire CSSF 18/698. Pour de plus amples informations, consultez notre dernière Newsletter 2/3 concernant les dispositions relatives aux délégations des GFI.

Le GFI peut également s'appuyer sur l'infrastructure informatique d'une société mère ou d'une de ses filiales, à condition que cette entité soit qualifiée et capable de fournir le service concerné. Dans ce cas, le GFI peut également s'appuyer sur la solution de « back-up » de cette entité à condition que la ségrégation des données du GFI soit assurée.

Infrastructure informatique en nuage

La circulaire CSSF 18/698 mentionne l'application de la circulaire 17/654 portant sur la sous-traitance informatique pour les GFI dans la mesure où le GFI a recours à une infrastructure informatique en nuage ou une infrastructure de « Cloud Computing ». Anciennement, la circulaire CSSF 17/654 était exclusivement applicable aux établissements de crédit, aux PSF, aux établissements de paiement et aux établissements de monnaie électronique.

Comme indiqué au point 26 de la circulaire CSSF 17/654, les GFI qui ont l'intention de recourir à une telle infrastructure doivent obtenir l'autorisation préalable de la CSSF, lorsque l'activité supportée par l'infrastructure de « Cloud Computing » est matérielle. Dans le cas contraire, une notification au préalable à la CSSF est suffisante.

Les GFI qui souhaitent mettre un terme à une sous-traitance informatique sur une infrastructure de « Cloud Computing » ; changer de fournisseur de services ; changer de modèles de service, doivent également le notifier à la CSSF.

Gouvernance informatique

La circulaire CSSF 18/698 souligne que les principes de gouvernance informatique doivent être intégrés dans le dispositif de gouvernance interne du GFI. Le GFI doit mettre en place un dispositif de gouvernance interne qui répond au concept des «trois lignes de défense».

La première ligne de défense est constituée par les unités opérationnelles. La seconde ligne de défense est formée par les fonctions permanentes de gestion des risques et de compliance qui contribuent au contrôle indépendant des risques, ainsi que par les fonctions de support, y compris **la fonction informatique** et la fonction comptable. Enfin, la troisième ligne de défense est constituée par la fonction d'audit interne qui effectue une évaluation indépendante, objective et critique des deux premières lignes de défense.

Les trois lignes de défense sont complémentaires. En effet, chaque ligne de défense assume ses responsabilités de contrôle indépendamment des autres lignes.

Plus d'informations

Joseph Stevens
ARCAD S.A.
11 rue des Trois Cantons
L-8399 WINDHOF
jstevens@arcad.lu