

FSMA_2023_24 du 12/10/2023

Guide pratique en matière d'externalisation

Champ d'application:

Le présent guide pratique s'adresse aux :

- sociétés de gestion de portefeuille et de conseil en investissement (ci-après la/les « SGPCI ») ;
- sociétés de gestion d'OPCVM/OPCA (ci-après la/les « SG »).

Résumé/Objectifs:

Ce guide pratique développe les principes de saine gestion en matière d'externalisation.

Structure:

1	Introduction	2
2	Principe de proportionnalité.....	3
3	Principes généraux régissant l'externalisation	4
3.1	Notion d'externalisation de fonctions	4
3.2	Fonctions visées et identification des fonctions critiques ou importantes	5
3.3	Externalisation intragroupe	7
4	Principes de saine gestion en matière d'externalisation	8
4.1	Cadre de gouvernance	8
4.1.1	Cadre global de gestion des risques	8
4.1.2	Responsabilité	8
4.1.3	Politique d'externalisation	10
4.1.4	Registre des externalisations.....	11
4.1.5	Conflits d'intérêts	12
4.1.6	Plan de poursuite de l'activité	12
4.1.7	Audit interne.....	13
4.2	Processus d'externalisation	13
4.2.1	Décision d'externaliser	13
4.2.1.1	Conditions de surveillance de l'externalisation	14
4.2.1.2	Evaluation des risques liés aux dispositifs d'externalisation.....	15
4.2.1.3	Sélection du prestataire de services	16
4.2.2	Contrat d'externalisation.....	17
4.2.3	Contrôle des fonctions externalisées	18
4.2.4	Stratégies de sortie.....	20
4.2.5	Notification à la FSMA en cas d'externalisation de fonctions critiques ou importantes	21
5	Conclusion.....	21

1 Introduction

Dans le cadre des efforts de rationalisation de son organisation, une SGPCI ou une SG peut être amenée à externaliser diverses fonctions qui pourraient contribuer - à différentes échelles - à la conduite de ses activités et à son bon fonctionnement.

Dans de bonnes conditions, l'externalisation peut contribuer à une meilleure gestion par le transfert de certaines fonctions à des tiers disposant d'une plus grande expertise et capables d'économies d'échelle accrues. Cependant, elle ne diminue en rien la responsabilité de la société de tenir compte des principes de saine gestion dans la conduite de ses activités. Il appartient dès lors, à l'organe d'administration de chaque SGPCI/SG, de mener une politique appropriée en matière d'externalisation de fonctions, en particulier en vue du maintien d'une organisation adéquate.

Disposer d'une organisation solide et adéquate est une condition essentielle d'agrément des SGPCI/SG¹. La FSMA contrôle que chaque SGPCI/SG est adéquatement organisée afin que les activités pour lesquelles elle est agréée soient exercées en conformité avec la législation applicable, en ce compris les activités qu'elle aurait externalisées. Le contrôle de cette organisation adéquate est la base du contrôle prudentiel exercé par la FSMA sur les SGPCI/SG.

Les réglementations applicables aux SGPCI/SG encadrent l'externalisation de certaines fonctions spécifiques, telles que la gestion du portefeuille d'investissement de l'OPC et la gestion discrétionnaire de portefeuille².

L'Autorité bancaire européenne (ABE) a publié des *Orientations*³ précisant les exigences légales similaires pour d'autres entreprises du secteur financier, tels que les établissements de crédit, et valant pour toute externalisation de fonction, qu'elle fasse ou non l'objet de règles légales spécifiques. L'ABE y spécifie les dispositifs en matière de gouvernance interne, y compris en termes de gestion saine des risques que ces établissements doivent mettre en œuvre lorsqu'ils externalisent des fonctions, en particulier en ce qui concerne l'externalisation de fonctions critiques ou importantes. Il s'agit d'un document de référence en matière d'externalisation.

S'appuyant entre autres sur les dispositions légales applicables en matière d'externalisation et ces *Orientations*, la FSMA développe dans le présent guide pratique les principes de saine gestion en matière d'externalisation de toute fonction.

¹ Art. 25 de la loi du 25 octobre 2016 relative à l'accès à l'activité de prestation de services d'investissement et au statut et au contrôle des sociétés de gestion de portefeuille et de conseil en investissement (ci-après « loi SGPCI »); art. 26 de la Loi OPCA; art. 201 de la Loi OPCVM et l'Arrêté royal du 12 novembre 2012 relatif aux sociétés de gestion d'organismes de placement collectif qui répondent aux conditions de la directive 2009/65/CE.

² Pour les SG, voir les art. 29 à 32 et 320 de la Loi OPCA, art. 202 Loi OPCVM et art. 75 et sv. du règlement délégué n° 231/2013 de la Commission du 19 décembre 2012 complétant la directive 2011/61/UE du Parlement européen et du Conseil en ce qui concerne les dérogations, les conditions générales d'exercice, les dépositaires, l'effet de levier, la transparence et la surveillance (ci-après « Règlement AIFM »). Pour les SGPCI, voir art. 25 de la loi SGPCI et les art. 30 et sv. du règlement délégué 2017/565 de la Commission du 25 avril 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles et les conditions d'exercice applicables aux entreprises d'investissement et la définition de certains termes aux fins de ladite directive (ci-après « Règlement MiFID II »).

³ Orientations relatives à l'externalisation (EBA/GL/2019/02) du 25 février 2019.

La FSMA est susceptible de faire évoluer ces principes en fonction notamment de bonnes ou mauvaises pratiques qu'elle constaterait dans le cadre de l'exercice de son contrôle des SGPCI/SG.

Le présent guide pratique s'applique sans préjudice des exigences particulières en matière d'externalisation à des prestataires de services en nuage⁴.

La circulaire PPB 2004/5 de la CBFA du 22 juin 2004 sur les saines pratiques de gestion en matière de sous-traitance par des établissements de crédit et des entreprises d'investissement est abrogée.

Les SGPCI/SG ont jusqu'au 30 juin 2024 pour mettre en œuvre le présent guide pratique et les principes de saine gestion qu'il contient.

2 Principe de proportionnalité⁵

L'organisation d'une SGPCI/SG doit être proportionnée à l'ampleur, la nature, l'échelle et la complexité de ses activités.

Les principes formulés dans le présent guide pratique en ce qui concerne l'externalisation de fonction doivent, le cas échéant, être interprétés à la lumière de ce principe de proportionnalité.

Le principe de proportionnalité signifie que le respect des exigences en matière d'externalisation de fonction est proportionnel à la nature, à la taille et à la complexité de l'organisation et des activités de la SGPCI/SG. Ainsi, lorsqu'elle se conforme à ces exigences, la SGPCI/SG doit également tenir compte de la complexité des fonctions externalisées, des risques découlant du dispositif d'externalisation, du caractère important ou critique de la fonction externalisée, ainsi que de l'incidence potentielle de l'externalisation sur la poursuite de ses activités.

Ce principe n'implique pas pour autant que la SGPCI/SG puisse être dispensée du respect de certaines exigences. Il en résulte, en revanche, que la manière dont la SGPCI/SG satisfait à ces exigences doit être appropriée à sa structure et à ses activités.

Pour la SGPCI/SG dont la structure, les activités et/ou les fonctions externalisées sont moins complexes, le principe de proportionnalité peut, par exemple, se concrétiser adéquatement en adoptant des politiques, des procédures et des mécanismes de contrôle interne simples.

Pour soutenir la mise en œuvre appropriée du présent guide pratique, la SGPCI/SG documente par écrit son analyse de proportionnalité (comply or explain).

⁴ Circulaire FSMA_2022_19 du 8/06/2022 – Mise en œuvre des orientations de l'ESMA relatives à la sous-traitance à des prestataires de services en nuage.

⁵ Art. 25, §2 de la loi SGPCI ; art. 201, §1 de la loi OPCVM ; art. 26 de la loi OPCA.

3 Principes généraux régissant l'externalisation

La SGPCI/SG peut faire appel à des prestataires de services. Elle est responsable du choix et du contrôle de l'activité des prestataires de services auxquels elle fait appel.

Le recours à des prestataires de services ne diminue en aucune façon la responsabilité de la SGPCI/SG. L'externalisation ne peut avoir pour effet de :

- compromettre la qualité du système de gouvernance de la SGPCI/SG ;
- accroître indûment le risque opérationnel ;
- compromettre le contrôle exercé par la FSMA ;
- nuire à la prestation continue d'un service professionnel à l'égard des clients.

3.1 Notion d'externalisation de fonctions

On entend par externalisation de fonctions tout appel fait à des tiers pour l'exercice de processus, de services ou d'activités propres à la SGPCI/SG.

L'externalisation fait, dès lors, référence au travail que la SGPCI/SG commande à un tiers, le prestataire de services, et qui est autrement réalisé par elle-même. Le travail peut impliquer, par exemple, une activité individuelle ou une série d'activités. En outre, la SGPCI/SG peut externaliser des travaux qui relèvent de nouvelles activités et qu'elle n'a dès lors pas effectués elle-même auparavant.

La situation dans laquelle un prestataire de services transfère lui-même une fonction externalisée à un autre prestataire de service constitue une sous-externalisation.

La SGPCI/SG peut faire appel à un prestataire de services sur la base d'un contrat de mandat ou d'un contrat d'entreprise au sens du Code civil. Une personne recevant mandat est chargée par une autre de poser un acte juridique. Le mandat confère donc un pouvoir de représentation. Dans le cadre d'un contrat d'entreprise, une personne est chargée de faire un ouvrage pour une autre, sans disposer du moindre pouvoir de représentation⁶. La notion d'externalisation vise donc tant des cas de délégation que de sous-traitance de fonctions.

La FSMA souligne que, ne relève pas de l'externalisation, l'appel à des tiers notamment pour :

- une fonction qui doit obligatoirement être exercée par un prestataire de services, tel que le contrôle légal des comptes ;
- les services d'information de marché (telle que la fourniture de données par Bloomberg,...) ;
- les services de correspondance bancaire ;
- l'acquisition de services qui, autrement, ne seraient pas assurés par la SGPCI/SG (tels que des conseils juridiques, le nettoyage, la sécurité et l'entretien des bâtiments,...).

⁶ Articles 1984, alinéa 1^{er}, et 1787 du Code civil.

3.2 Fonctions visées et identification des fonctions critiques ou importantes

Le présent guide pratique vise l'externalisation de toute fonction, définie comme tout processus, service ou activité.

Cependant, il y a lieu de porter une attention particulière à l'externalisation de fonctions devant être considérées comme critiques ou importantes.

Il revient à la SGPCI/SG de juger si une fonction est critique ou importante. A cette fin, elle doit répondre à la question de savoir si la fonction concernée est d'une importance essentielle pour la conduite de ses affaires.

Une fonction est considérée comme critique ou importante si sa suppression, une anomalie ou une défaillance dans son exécution est susceptible de nuire sérieusement :

- à la capacité de la société de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables de la législation applicable ;
- à ses performances financières ;
- à la solidité ou la continuité de ses services et activités.

La FSMA estime que :

- les fonctions de gestion collective des OPC(A) et les services d'investissement doivent dans tous les cas être considérées comme des fonctions critiques ou importantes. La FSMA rappelle que la SGPCI/SG doit conserver en permanence une substance suffisante et ne pas devenir une « coquille vide » ou une « société boîte aux lettres »⁷ ;
- les fonctions de contrôle indépendantes sont également critiques ou importantes eu égard au rôle qu'elles jouent dans la structure de contrôle interne de la SGPCI/SG.

A cet égard, la FSMA rappelle que l'externalisation de ces fonctions ne peut cependant impliquer leur transfert dans leur intégralité au prestataire de services ni affaiblir la permanence du contrôle interne de la SGPCI/SG ou son effectivité. Par conséquent, l'externalisation sera proportionnée et limitée aux tâches opérationnelles de ces fonctions⁸.

Lorsque la SGPCI/SG évalue si un dispositif d'externalisation se rapporte à une fonction critique ou importante, elle doit veiller à prendre en considération, outre les résultats de l'évaluation des risques liés au dispositif lui-même, au moins les facteurs suivants :

- si le dispositif d'externalisation est directement lié à la fourniture d'activités ou de services pour lesquels la SGPCI/SG est agréée ;
- l'incidence potentielle de toute perturbation de la fonction externalisée ou de l'incapacité du prestataire de services à assurer le service aux niveaux de service convenus de manière continue en prenant en compte les éléments suivants :
 - sa résilience et sa viabilité financière à court et à long terme,
 - la poursuite de l'activité et la résilience opérationnelle,

⁷ Art. 31, al. 2 de la loi OPCA, art. 82 du Règlement AIFM.

⁸ V. Circulaire FSMA_2013_08 du 23/04/2013 « Fonction de compliance ».

- les risques opérationnels, y compris les risques liés à la conduite, aux technologies de l'information et de la communication et les risques juridiques,
- le risque de réputation,
- le cas échéant, la planification du redressement et la continuité opérationnelle dans une situation d'intervention précoce ;
- l'incidence potentielle du dispositif d'externalisation sur sa capacité :
 - à identifier, suivre et gérer tous les risques,
 - à se conformer à toutes les exigences légales et réglementaires,
 - à effectuer les audits appropriés concernant la fonction externalisée ;
- l'incidence potentielle sur les services fournis à ses clients ;
- tous les dispositifs d'externalisation, l'exposition globale de la SGPCI/SG à un même prestataire de services et l'incidence cumulative potentielle des dispositifs d'externalisation dans un même domaine d'activité ;
- la taille et la complexité de tout domaine d'activité touché ;
- la possibilité que le dispositif d'externalisation proposé puisse être étendu sans remplacer ou réviser l'accord sous-jacent ;
- la capacité de transférer le dispositif d'externalisation proposé vers un autre prestataire de services, si nécessaire ou souhaitable, tant sur le plan contractuel que dans la pratique, y compris les risques estimés, les obstacles à la poursuite de l'activité, les coûts et le délai nécessaire pour procéder au transfert (« substituabilité ») ;
- la capacité d'internaliser la fonction externalisée dans la SGPCI/SG, si nécessaire ou souhaitable ;
- la protection des données et l'impact potentiel d'une violation de la confidentialité ou d'un manquement à l'obligation de garantir la disponibilité et l'intégrité des données sur la SGPCI/SG et ses clients, notamment, mais non exclusivement, le respect du règlement GDPR⁹.

La SGPCI/SG doit réévaluer, selon ses propres procédures, régulièrement la qualification de chaque fonction externalisée afin de déterminer s'il y a lieu de (continuer à) la considérer comme critique ou importante. La SGPCI/SG documente son analyse.

⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

3.3 Externalisation intragroupe

L'externalisation intragroupe n'est pas nécessairement moins risquée que l'externalisation vers une entité extérieure au groupe.

La FSMA souligne, dès lors, que l'externalisation intragroupe est soumise au même cadre réglementaire et aux mêmes conditions que l'externalisation vers des prestataires de services extérieurs au groupe.

Lorsqu'une SGPCI/SG a l'intention d'externaliser des fonctions auprès d'une entité du groupe, elle doit s'assurer que le choix de cette entité est fondé sur des raisons objectives. En particulier, le contrat d'externalisation ne doit pas exposer la SGPCI/SG à un conflit d'intérêts injustifié (cf. [section 4.1.5](#)). La rémunération éventuellement versée pour les services fournis doit faire l'objet d'une attention particulière. Elle devrait être fixée aux conditions du marché et justifiée eu égard à la quantité et la complexité des fonctions externalisées.

Lorsqu'elle fait partie d'un groupe, la SGPCI/SG pourrait prendre en compte dans son évaluation des risques le fait qu'elle peut bénéficier, auprès d'entités du groupe, d'une centralisation du suivi opérationnel de l'externalisation. Elle ne peut toutefois pas s'en remettre exclusivement à des entités du groupe pour la gestion de l'externalisation.

La SGPCI/SG doit concevoir des procédures pour l'exécution d'un suivi et d'une surveillance appropriés afin de garantir le respect des exigences réglementaires et énoncées dans le présent guide pratique.

La SGPCI/SG doit être en mesure d'assurer le suivi indépendant du prestataire de services, notamment en recevant, au moins une fois par an et sur demande, de la part de la fonction de suivi centralisé, des rapports comprenant, au minimum, un résumé de l'évaluation des risques et du suivi des performances et en posant un regard critique sur ces rapports. En outre, la SGPCI/SG doit recevoir de la part de la fonction de suivi centralisé un résumé des rapports d'audit pertinents sur l'externalisation et, sur demande, le rapport d'audit complet.

La SGPCI/SG doit veiller à être dûment informée des changements prévus concernant les prestataires de services qui sont surveillés de manière centralisée et de l'impact potentiel de ces changements sur les fonctions exercées. La SGPCI/SG devrait recevoir un résumé de l'analyse des risques, incluant les risques juridiques, de conformité aux exigences réglementaires et l'impact sur les niveaux de service, afin de pouvoir évaluer l'impact de ces changements et les accepter ou prendre les mesures qui s'imposent.

La SGPCI/SG doit déterminer si l'étendue et le contenu de ces rapports et informations sont cohérents et appropriés et prendre des mesures s'ils ne lui permettent pas de se conformer aux exigences réglementaires et contenues dans le présent guide pratique.

Lorsque la SGPCI/SG s'appuie sur des plans de continuité d'activité établis au niveau du groupe concernant ses fonctions externalisées, elle doit s'assurer que ces plans sont conformes aux dispositions des [sections 4.1.6](#) et [4.2.4](#).

4 Principes de saine gestion en matière d'externalisation

La SGPCI/SG doit veiller à répondre, dans tous les cas, aux principes ci-dessous lorsqu'elle externalise des fonctions critiques ou importantes, et qu'elle s'y conforme de manière proportionnelle lorsqu'elle confie des fonctions autres à des tiers.

4.1 Cadre de gouvernance

4.1.1 Cadre global de gestion des risques

Dans le cadre du dispositif de contrôle interne d'ensemble, y compris les mécanismes de contrôle interne, la SGPCI/SG doit disposer d'un cadre global de gestion des risques à l'échelle de l'établissement, s'étendant à toutes les activités et unités internes. Dans ce cadre, la SGPCI/SG doit identifier et gérer tous les risques auxquels elle est exposée, y compris les risques résultant d'arrangements avec des tiers. Le cadre de la gestion des risques doit également permettre à la SGPCI/SG de prendre des décisions éclairées en matière de prise de risques et de veiller à ce que les mesures de gestion des risques soient mises en œuvre de façon appropriée, notamment en ce qui concerne les cyber-risques.

La SGPCI/SG, compte tenu du principe de proportionnalité, doit identifier, évaluer, surveiller et gérer tous les risques auxquels elle est ou pourrait être exposée dans le cadre d'arrangements conclus avec des tiers, qu'il s'agisse ou non d'accords d'externalisation. Les risques, en particulier les risques opérationnels, de tous les arrangements conclus avec des tiers, doivent être évalués conformément à la [section 4.2.1.2](#).

Dans un contexte de groupe, lorsque la SGPCI/SG s'appuie sur une évaluation centrale préalable à l'externalisation d'une fonction, elle doit veiller à recevoir un résumé de l'évaluation et s'assurer que celle-ci prend suffisamment en compte sa structure et ses risques spécifiques afin de pouvoir décider en connaissance de cause de procéder ou non à l'externalisation envisagée.

4.1.2 Responsabilité

La SGPCI/SG qui externalise des fonctions reste entièrement responsable du respect de ses engagements et obligations légales notamment vis-à-vis de ses clients et de la FSMA¹⁰.

Ceci signifie que l'organe d'administration de la SGPCI/SG répond totalement de l'élaboration des politiques et du contrôle portant sur l'ensemble des tâches externalisées. Cet organe doit prendre soin d'identifier et gérer tous les risques qui y sont inhérents, et en particulier les risques opérationnels.

L'organe d'administration conserve donc en permanence l'entière responsabilité pour au moins :

- s'assurer que la SGPCI/SG satisfait en permanence aux conditions de son agrément ;
- l'organisation interne de la SGPCI/SG ;
- l'identification, l'évaluation et la gestion des conflits d'intérêts ;

¹⁰ Art. 31, §1, a) du Règlement MiFID II ; art. 202, §1, 3° de la loi OPCVM ; art. 29, §1, 6° de la loi OPCA ; Art. 75, al. 1, a) du Règlement AIFM.

- la définition des stratégies et politiques de la SGPCI/SG (par ex. le modèle de risques, l'appétit aux risques, le cadre de la gestion des risques) ;
- la surveillance de la gestion quotidienne de la SGPCI/SG, y compris la gestion de tous les risques associés à l'externalisation ;
- le rôle de contrôle de l'organe d'administration dans sa fonction de surveillance, y compris de supervision et de contrôle du processus décisionnel de la direction.

Ainsi, la SGPCI/SG doit au moins veiller :

- à pouvoir prendre et mettre en œuvre les décisions relatives à ses activités et à ses fonctions critiques ou importantes, y compris celles qui ont été externalisées ;
- à maintenir la régularité de ses activités ;
- à identifier, évaluer, gérer et atténuer adéquatement les risques liés aux dispositifs d'externalisation actuels et prévus ;
- à mettre en place des dispositifs de confidentialité appropriés en ce qui concerne les données et autres informations ;
- à faire circuler l'information avec les prestataires de services ;
- à avoir la possibilité d'entreprendre au moins l'une des actions suivantes dans un délai approprié :
 - transférer la fonction vers d'autres prestataires de services,
 - internaliser la fonction,
 - interrompre les activités qui dépendent de la fonction ;
- à mettre en œuvre des mesures appropriées lorsque des données à caractère personnel sont traitées par des prestataires de services situés dans l'UE et/ou dans des pays tiers, et à traiter les données conformément au règlement (UE) 2016/679¹¹.

La SGPCI/SG doit veiller à :

- conserver l'expérience, les connaissances et les ressources nécessaires pour assurer une gestion et un contrôle approprié des dispositifs d'externalisation et pour y apporter, au besoin, les ajustements qui s'imposent ;
- adopter des méthodes de suivi et des reporting adaptés à la nature des fonctions externalisées et aux risques qui y sont liés. La SGPCI/SG prévoira également, à cet effet, des moyens de communication clairs, assortis d'une obligation pour le prestataire de services de signaler tout problème ayant un impact sur les activités externalisées, ainsi que toute situation d'urgence ;
- attribuer clairement, en interne, les responsabilités en matière de mise en place et de suivi des dispositifs d'externalisation.

¹¹ Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), (ci-après « Règlement GDPR »).

4.1.3 Politique d'externalisation

La SGPCI/SG, qui envisage d'avoir recours à l'externalisation, doit établir sa politique d'externalisation par écrit. L'organe d'administration approuve ladite politique.

La SGPCI/SG englobe dans cette politique sa stratégie, ainsi que les lignes de force s'appliquant aux processus d'externalisation qu'elle suivra tout au long du contrat. La SGPCI/SG porte une attention particulière aux éléments suivants :

- le maintien des responsabilités ;
- la définition des exigences relatives aux dispositifs d'externalisation ;
- les principes permettant de déterminer si une fonction est critique ou importante (cf. [section 3.2](#)) ;
- l'identification, l'évaluation et la gestion des risques liés aux dispositifs d'externalisation (cf. [section 4.2.1.2](#)) ;
- le processus d'approbation des nouveaux dispositifs d'externalisation et les pouvoirs internes en matière de signature de contrats d'externalisation (cf. [section 4.2.1](#)) ;
- la participation des fonctions de contrôle indépendantes dans les dispositifs d'externalisation ;
- la procédure de sélection du prestataire de services (cf. [section 4.2.1.3](#)) ;
- les éléments à inclure dans le contrat d'externalisation (cf. [section 4.2.2](#)) ;
- les procédures d'identification, d'évaluation, de gestion et d'atténuation des conflits d'intérêts potentiels (cf. [section 4.1.5](#)) ;
- la mesure dans laquelle la SGPCI/SG accepte que le prestataire de service externalise, à son tour, certaines fonctions (sous-externalisation en cascade) et les conditions générales applicables dans un tel cas ;
- la méthode et la fréquence d'évaluation des prestations et des résultats des prestataires de services (cf. [section 4.2.3](#)) ;
- la continuité et les plans d'urgence, incluant les stratégies de sortie (cf. [sections 4.1.6](#) et [4.2.4](#)) ;
- l'intégrité et la confidentialité des données (surtout dans le cas de la gestion de données) ;
- le respect du cadre légal et réglementaire.

La SGPCI/SG doit veiller à traduire les principes ci-dessus en procédures de mise en œuvre, de contrôle et de reporting.

La politique d'externalisation devrait établir une distinction entre les éléments suivants :

- l'externalisation de fonctions critiques ou importantes et les autres dispositifs d'externalisation (cf. [section 3.2](#)) ;
- les dispositifs d'externalisation intragroupe et l'externalisation à des entités extérieures au groupe (cf. [section 3.3](#)) ;
- l'externalisation à des prestataires de services agréés par une autorité compétente et l'externalisation à ceux qui ne le sont pas ;

- l'externalisation à des prestataires de services situés dans un État membre ou dans un pays tiers. La SGPCI/SG doit examiner régulièrement et mettre à jour sa politique d'externalisation.

4.1.4 Registre des externalisations

La SGPCI/SG doit veiller à tenir un registre reprenant des informations sur toutes les externalisations mises en place, en faisant une distinction entre l'externalisation de fonctions critiques ou importantes et l'externalisation d'autres fonctions.

Le registre devrait contenir, au moins, les informations suivantes pour toutes les externalisations en cours :

- un numéro de référence pour chaque externalisation ;
- la date de début et, le cas échéant, la prochaine date de renouvellement du contrat, la date de fin et/ou les délais de préavis pour le prestataire de services et pour la SGPCI/SG ;
- une brève description de la fonction externalisée, y compris les données qui sont externalisées et la confirmation (ou non) que des données à caractère personnel (par ex., en indiquant oui ou non dans un champ de données séparé) ont été transférées ou si leur traitement est externalisé vers un prestataire de services ;
- une catégorie attribuée par la SGPCI/SG qui reflète la nature de la fonction visée au point précédent (tels que gestion du portefeuille d'investissement de l'OPC(A), conseil en investissement, technologie de l'information, fonction de contrôle), ce qui devrait faciliter l'identification des différents types de dispositifs ;
- le nom du prestataire de services, le numéro d'immatriculation de la société, l'identifiant de la personne morale (si disponible), le siège social et autres coordonnées pertinentes, ainsi que le nom de son entreprise mère (le cas échéant) ;
- le(s) pays au sein duquel ou desquels le service sera exécuté, y compris la localisation (c.-à-d. le pays ou la région) des données ;
- si (oui/non) la fonction externalisée est considérée comme critique ou importante, avec un bref résumé des raisons pour lesquelles la fonction externalisée est considérée comme critique ou importante ;
- en cas d'externalisation vers un prestataire de services en nuage, les modèles de services et de déploiement en nuage, c.-à-d. en nuage public/privé/hybride/communautaire, et la nature spécifique des données conservées et les lieux (c.-à-d. les pays ou régions) où ces données seront stockées ;
- la date de la dernière évaluation du caractère critique ou important de la fonction externalisée ;
- la législation applicable au contrat et le tribunal compétent.

Pour l'externalisation de fonctions critiques ou importantes, le registre devrait comprendre au moins les informations complémentaires suivantes:

- la date de l'évaluation des risques la plus récente et un bref résumé des principaux résultats ;
- les dates des derniers audits et des prochains audits prévus, le cas échéant ;

- le nom des éventuels prestataires de services de nième rang, auxquels des parties significatives d'une fonction sont sous-externalisées, y compris le pays où les prestataires de services de nième rang sont enregistrés, où le service sera exécuté et, le cas échéant, le lieu (c.-à-d. le pays ou la région) où les données seront stockées ;
- le résultat de l'évaluation de la substituabilité du prestataire de services (facile, difficile ou impossible), la possibilité d'internaliser une fonction dans l'établissement, ou l'impact d'une interruption de la fonction ;
- l'identification de prestataires de services alternatifs ;
- le coût budgétaire annuel estimé.

La SGPCI/SG doit être en mesure de mettre à la disposition de la FSMA, et à sa première demande, le registre complet ou des parties déterminées de celui-ci, sous une forme exploitable par ordinateur.

4.1.5 Conflits d'intérêts¹²

Les activités d'une SGPCI/SG se caractérisent par le concours de nombreux intérêts, souvent convergents mais tout aussi souvent divergents ou conflictuels, qui exigent un encadrement adéquat. Ces conflits d'intérêts peuvent notamment être liés aux dispositifs d'externalisation que la SGPCI/SG a mis en place.

La mise en place et le maintien d'une bonne gouvernance impliquent que la SGPCI/SG prenne des mesures adéquates pour la gestion de ces conflits d'intérêts.

Par conséquent, sans préjudice de l'application de dispositions légales spécifiques, la SGPCI/SG doit identifier et prévenir ces conflits d'intérêts ou, si cela s'avère raisonnablement impossible, les gérer d'une façon qui ne nuise pas aux intérêts des clients.

4.1.6 Plan de poursuite de l'activité¹³

La SGPCI/SG doit mettre en œuvre tous les moyens raisonnables pour exercer ses activités sans interruption. Tenant compte du principe de proportionnalité, elle doit plus précisément veiller à ce que son organisation, ses systèmes et ses procédures soient conçus de manière telle qu'en cas d'interruption sérieuse et non planifiée de ses activités, elle puisse continuer à remplir ses obligations résultant de son statut réglementé et préserver les intérêts et les droits de ses clients. Ces exigences valent également en cas d'externalisation de fonctions.

La SGPCI/SG doit mettre en place, maintenir et tester périodiquement des plans appropriés de poursuite de l'activité pour les fonctions critiques ou importantes externalisées.

Les plans de poursuite de l'activité devraient tenir compte de l'éventualité selon laquelle la qualité de la fourniture de la fonction externalisée pourrait se dégrader de manière inacceptable ou être défaillante. Ces plans devraient également tenir compte de l'incidence potentielle de l'insolvabilité ou d'autres défaillances des prestataires de services et, le cas échéant, des risques politiques liés à la juridiction du prestataire de services¹⁴.

¹² Voir art. 80 du Règlement AIFM ; art. 202, §1^{er}, 4^o, c) de la loi OPCVM ; art. 30, al. 1, 2^o et 37 de la loi OPCA ; art. 34, §2, a) du Règlement MiFID II.

¹³ Voir art. 75, al. 1, g) du Règlement AIFM ; art. 31, §2, l) du Règlement MiFID II.

¹⁴ Il est également renvoyé au point 3.3, *in fine*, quant à la possibilité pour la SGPCI/SG de s'appuyer sur des plans de continuité établis au niveau du groupe.

4.1.7 Audit interne¹⁵

La SGPCI/SG doit veiller à ce que les activités de la fonction d'audit interne couvrent, selon une « risk-based approach », l'examen indépendant des fonctions externalisées. Le plan et le programme d'audit devraient comprendre, en particulier, la révision des dispositifs d'externalisation de fonctions critiques ou importantes.

En ce qui concerne le processus d'externalisation, la fonction audit interne devrait au moins s'assurer :

- que le cadre d'externalisation de la SGPCI/SG, y compris la politique d'externalisation, est correctement et effectivement mis en œuvre et est conforme aux lois et règlements applicables, à la stratégie en matière de risques, ainsi qu'aux décisions de l'organe d'administration ;
- de l'adéquation, la qualité et l'efficacité de l'évaluation du caractère critique ou important des fonctions ;
- de l'adéquation, la qualité et l'efficacité de l'évaluation des risques liés aux dispositifs d'externalisation et que ces risques restent conformes avec la stratégie de la SGPCI/SG en matière de risques ;
- que le niveau de participation des organes de gouvernance est approprié ;
- que le suivi et la gestion des dispositifs d'externalisation sont appropriés.

4.2 Processus d'externalisation

4.2.1 Décision d'externaliser¹⁶

La SGPCI/SG doit appuyer les décisions d'externaliser une fonction, et de désigner un prestataire de services, sur une analyse approfondie et documentée et elle doit vérifier qu'elle respecte sa politique d'externalisation.

La FSMA souligne combien il est important de documenter la procédure d'examen menée lors de l'externalisation d'une fonction et du choix d'un prestataire de services, et en particulier la décision d'engagement proprement dite et les considérations qui l'ont motivée. La conservation de cette documentation doit également faire l'objet de toute l'attention voulue.

Avant d'externaliser une fonction, la SGPCI/SG doit veiller à :

- évaluer si le dispositif d'externalisation concerne une fonction critique ou importante (cf. [section 3.2](#)) ;
- évaluer si les conditions de surveillance de l'externalisation énoncées sont remplies (cf. [section 4.2.1.1](#)) ;

¹⁵ Voir art. 25, §1, 4° de la loi SGPCI ; art. 24 du Règlement MiFID II ; art. 201 de la loi OPCVM ; art. 62 du Règlement AIFM.

¹⁶ Voir art. 202, §1, 1° de la loi OPCVM ; art. 29, §1, 1° de la loi OPCA ; art. 76 du Règlement AIFM ; art. 26, §4 de la loi SGPCI.

- identifier et évaluer tous les risques pertinents du dispositif d'externalisation (cf. [section 4.2.1.2](#)) ;
- effectuer les vérifications nécessaires à l'égard du prestataire de services potentiel (cf. [section 4.2.1.3](#)) ;
- identifier et évaluer les conflits d'intérêts que l'externalisation pourrait entraîner (cf. [section 4.1.5](#)).

4.2.1.1 Conditions de surveillance de l'externalisation¹⁷

Si une fonction est externalisée auprès d'un prestataire de services situé dans un état membre de l'espace économique européen et que son exécution requiert un agrément ou un enregistrement, la SGPCI/SG doit s'assurer que le prestataire de services est dûment agréé ou enregistré par l'autorité compétente.

Si une fonction est externalisée auprès d'un prestataire de services situé dans un pays tiers et que son exécution requiert un agrément ou un enregistrement, la SGPCI/SG doit s'assurer¹⁸ :

- que le prestataire de services est dûment agréé ou enregistré et surveillé par l'autorité compétente ;
- qu'il existe un accord de coopération entre la FSMA et l'autorité de contrôle chargée de la surveillance du prestataire de services. L'accord de coopération devrait garantir que la FSMA est en mesure :
 - d'obtenir, sur demande, les informations nécessaires à l'accomplissement de ses missions de surveillance¹⁹,
 - d'obtenir un accès approprié aux données, documents, locaux ou personnel du pays tiers qui sont pertinents pour l'exercice de son pouvoir de surveillance,
 - de recevoir, dès que possible, des informations de l'autorité de contrôle du pays tiers pour enquêter sur des manquements manifestes aux exigences légales,
 - de coopérer avec l'autorité de contrôle compétente du pays tiers, en ce qui concerne l'application de la législation en cas de manquement aux exigences réglementaires applicables et de violation de la législation nationale belge. La coopération devrait inclure, sans nécessairement s'y limiter, la réception, dès que possible, d'informations sur les éventuels manquements aux exigences réglementaires applicables de la part de l'autorité de contrôle du pays tiers.

¹⁷ Voir art. 78, §2, e) du Règlement AIFM ; art. 31 du Règlement MiFID II.

¹⁸ Voir art. 202, §1, 6° de la loi OPCVM ; art. 29, §1, 5° de la loi OPCA ; art. 32, §1, a) du Règlement MiFID II.

¹⁹ Conformément à la directive Ucits (2009/65/CE), la directive AIFM (2011/61/UE), la directive MiFID II (2014/65/UE) ainsi que les règlements délégués européens les complétant (2017/565 et 231/2013), les lois belges transposant ces directives ainsi que leurs arrêtés d'exécution.

4.2.1.2 Evaluation des risques liés aux dispositifs d'externalisation²⁰

Avant d'externaliser une fonction, la SGPCI/SG doit veiller à :

- définir les effets attendus de l'externalisation, avec une estimation coûts-bénéfices ;
- évaluer les risques financiers, opérationnels (tels que les cyber-risques), réglementaires et d'atteinte à sa réputation et prendre en considération les résultats de cette évaluation lorsqu'elle décide si une fonction doit être externalisée. L'évaluation devrait inclure, le cas échéant, des scénarios d'évènements de risque potentiel, y compris des évènements de risque potentiel très élevé. Dans ce cadre, la SGPCI/SG devrait évaluer l'impact potentiel de services défaillants ou inadéquats, y compris les risques causés par les processus, systèmes, personnes ou évènements externes ;
- prendre les mesures appropriées pour prévenir tout risque opérationnel supplémentaire indu ;
- examiner les conséquences du lieu d'implantation du prestataire de services (dans ou en-dehors de l'espace économique européen) dont :
 - les limites en matière de contrôle liées aux pays où les fonctions sont externalisées ou pourraient être exercées et où les données sont stockées ou susceptibles de l'être,
 - la stabilité politique et la situation en matière de sécurité des juridictions, y compris :
 - les lois en vigueur, et notamment les lois sur la protection des données,
 - les dispositions en vigueur en matière d'application des lois,
 - les dispositions de la loi sur l'insolvabilité qui s'appliqueraient en cas de défaillance d'un prestataire de services et les contraintes qui pourraient apparaître en ce qui concerne la récupération urgente des données de la SGPCI/SG en particulier ;
- définir un niveau approprié de protection de la confidentialité des données, de poursuite des fonctions externalisées, ainsi que d'intégrité et de traçabilité des données et des systèmes dans le cadre de l'externalisation envisagée. La SGPCI/SG devrait également envisager la mise en place de mesures spécifiques, le cas échéant, applicables aux données en transit, aux données en mémoire et aux données au repos, telles que l'utilisation de technologies de cryptage associées à une architecture de gestion des clés appropriée ;
- évaluer les risques de continuité, notamment :
 - les risques de concentration²¹ et de dépendance susceptibles de survenir lorsque des fonctions importantes sont en grande partie confiées à un même prestataire de services difficilement substituable ou lorsque des accords d'externalisation multiples sont conclus avec un même prestataire de services ou des prestataires de services étroitement liés,
 - les mesures de précaution à prendre afin que la fonction externalisée puisse être confiée à un autre prestataire de services ou gérée en interne, au cas où la continuité ou la qualité de la prestation de services risquerait d'être compromise ;

²⁰ Voir art. 26, §4 de la loi SGPCI ; art. 31, §2, e) du Règlement MiFID II ; art. 202, §5 de la loi OPCVM ; art. 75, al. 1, f) du Règlement AIFM.

²¹ A noter que ce risque est également susceptible d'impacter d'autres risques, tel que le risque de conflits d'intérêts, par exemple lorsque le prestataire de services fait partie du même groupe et que des fonctions importantes lui sont en grande partie confiées.

- examiner si le prestataire de services est une filiale ou une entreprise mère, s'il est inclus dans le périmètre de consolidation comptable et, si tel est le cas, la mesure dans laquelle la SGPCI/SG contrôle le prestataire de services ou peut exercer une influence sur ses actions.

En cas de sous-externalisation en cascade, la SGPCI/SG prend les précautions nécessaires pour pouvoir évaluer à l'avance et avec précision les conséquences d'une telle décision et vérifier que celle-ci ne compromet pas le respect des dispositions légales et contractuelles.

La SGPCI/SG doit veiller à documenter l'analyse effectuée et ses résultats et estimer dans quelle mesure le dispositif d'externalisation augmenterait ou réduirait le risque opérationnel.

4.2.1.3 Sélection du prestataire de services²²

Avant de conclure un accord d'externalisation, la SGPCI/SG doit veiller à ce que le prestataire de services possède toutes les qualités requises pour exercer la fonction critique ou importante externalisée de manière fiable et professionnelle, de façon à satisfaire à ses obligations pendant toute la durée du contrat.

A cette fin, la SGPCI/SG s'assure que le prestataire de services dispose au minimum de(s):

- l'honorabilité professionnelle ;
- capacités appropriées et suffisantes ;
- l'expertise nécessaire (qualifications et expérience professionnelles) ;
- ressources suffisantes (notamment humaines, informatiques, financières) ;
- la structure organisationnelle adéquate.

La SGPCI/SG doit veiller également :

- au respect de sa politique d'intégrité, en accordant une attention particulière aux mesures prises par le prestataire de services pour éviter les conflits d'intérêts réels ou potentiels vis-à-vis de la SGPCI/SG et de toutes les parties concernées et, le cas échéant, dûment les gérer ;
- à l'appréciation de la politique de continuité du prestataire de services, y compris des plans d'urgence au regard de ses propres exigences de continuité ;
- à la conformité des exigences du prestataire de services en matière de sécurité et de confidentialité de l'information avec ses propres exigences ;
- à ce que les principaux éléments de la politique de rémunération du prestataire de services ne contreviennent pas aux principes généraux de sa politique de rémunération ;
- au respect du cadre législatif régissant ses activités et de la législation en matière de protection des données (RGPD).

D'autres facteurs peuvent également être pris en compte, telles que les relations à long terme avec le prestataire de services, la circonstance qu'il fait ou non partie du même groupe, et qu'il soit ou non surveillé par une autorité de contrôle.

Enfin, la SGPCI/SG devrait prendre les mesures appropriées pour veiller à ce que les prestataires de services agissent conformément à leurs valeurs et à leur code de conduite. En particulier, en ce qui concerne les prestataires de services situés dans des pays tiers et, le cas échéant, leurs sous-traitants. La SGPCI/SG devrait s'assurer que le prestataire de services agit d'une manière éthique et socialement

²² Voir art. 77 du Règlement AIFM ; art. 31, §2, a) du Règlement MiFID II.

responsable et respecte les normes internationales relatives aux droits de l'homme (par ex. la Convention européenne des droits de l'homme), à la protection de l'environnement et à la mise en place de conditions de travail appropriées, notamment l'interdiction du travail des enfants.

4.2.2 Contrat d'externalisation²³

La SGPCI/SG conclut une convention écrite avec le prestataire de services.

La FSMA souligne que la SGPCI/SG doit veiller à ce qu'il y ait cohérence entre le contrat d'externalisation et les autres documents relatifs à ses activités, telles que ses politiques.

La SGPCI/SG doit mettre à jour les contrats d'externalisation et/ou leurs annexes (telles que la liste des collaborateurs internes de la SGPCI/SG autorisés à donner des instructions au prestataire de services) chaque fois que des changements significatifs se produisent.

Compte tenu de leur faible valeur probante, les accords verbaux conclus avec des prestataires de services devraient toujours être confirmés par écrit ou formalisés d'une autre manière.

Les contrats d'externalisation, portant sur des fonctions critiques ou importantes, devraient au moins comporter les points suivants :

- une description claire de la fonction externalisée ;
- la date de début et de fin du contrat, le cas échéant, et les modalités de prolongation ainsi que les délais de préavis pour le prestataire de services et la SGPCI/SG ;
- la législation applicable au contrat et le tribunal compétent ;
- les obligations financières des parties ;
- les conditions auxquelles le prestataire de services peut, à son tour, sous-externaliser des fonctions qui lui ont été confiées, et la clause prévoyant que toute externalisation en cascade se fera sans préjudice des devoirs et responsabilités incombant au prestataire de services ;
- en cas de sous-externalisation d'une partie de fonction critique ou importante, si (oui/non) la partie sous-externalisée est considérée comme critique ou importante ;
- l'obligation du prestataire de services d'informer la SGPCI/SG de toute sous-externalisation prévue ;
- le droit de la SGPCI/SG de s'opposer à la sous-externalisation envisagée, ou aux changements significatifs la concernant ;
- le droit de la SGPCI/SG de résilier l'accord de sous-externalisation abusive, par exemple, lorsqu'elle augmente sensiblement les risques pour la SGPCI/SG ;
- en cas de sous-externalisation, l'obligation du prestataire de services de contrôler de manière appropriée, les prestataires de services de même rang, conformément à la politique définie par la SGPCI/SG ;
- en cas de sous-externalisation, l'obligation du prestataire de services d'obtenir l'engagement du prestataire de services de même rang de :
 - se conformer à toutes les lois, exigences réglementaires et obligations contractuelles applicables,

²³ Voir notamment : art. 75, al. 1, h) du Règlement AIFM ; art. 31, §3 du Règlement MiFID II.

- accorder à la SGPCI/SG et à la FSMA les mêmes droits d'accès et d'audit que ceux qu'il a lui-même accordés ;
- le(s) lieu(x) (c.-à-d. les régions ou pays) où la fonction sera assurée et/ou où les données pertinentes seront conservées et traitées, y compris le lieu de stockage éventuel, et les conditions à remplir, y compris l'obligation d'informer la SGPCI/SG si le prestataire de services envisage de modifier le(s) lieu(x) ;
- le cas échéant, les dispositions concernant l'accessibilité, la disponibilité, l'intégrité, la confidentialité et la sécurité des données pertinentes ;
- le droit de la SGPCI/SG de contrôler en permanence les performances du prestataire de services ;
- les niveaux de service convenus, qui devraient inclure des objectifs de performance quantitatifs et qualitatifs précis pour la fonction externalisée afin de permettre un suivi en temps utile, de sorte que des mesures correctives appropriées puissent être prises dans les meilleurs délais si les niveaux de service convenus ne sont pas respectés ;
- les modalités d'échange d'informations et les obligations de reporting du prestataire de services ;
- l'obligation pour le prestataire de services de signaler tout évènement susceptible d'avoir un impact significatif sur sa capacité ou, en cas de sous-externalisation, celle d'un prestataire de services de même rang à exercer les fonctions externalisées de manière efficace et conforme au cadre légal et réglementaire applicable ;
- si le prestataire de services doit souscrire une assurance obligatoire contre certains risques et, le cas échéant, le niveau de couverture d'assurance demandé ;
- l'obligation du prestataire de services de mettre en œuvre et tester des plans d'urgence de continuité ;
- des dispositions garantissant l'accès aux données appartenant à la SGPCI/SG en cas d'insolvabilité ou d'interruption des activités commerciales du prestataire de services ;
- l'obligation pour le prestataire de services de coopérer avec la FSMA et de répondre directement à ses questions en rapport avec les fonctions externalisées ;
- le droit inconditionnel de la SGPCI/SG d'inspecter et d'auditer le prestataire de services en ce qui concerne, en particulier, la fonction critique ou importante externalisée. La SGPCI/SG est tenue d'exercer ce droit en « bon père de famille »²⁴ ;
- les droits de résiliation.

4.2.3 Contrôle des fonctions externalisées²⁵

La SGPCI/SG doit effectuer, l'accent étant mis sur l'externalisation des fonctions critiques ou importantes, le suivi permanent des performances des prestataires de services en ce qui concerne tous les dispositifs d'externalisation selon une « risk-based approach », en veillant notamment à garantir la disponibilité, l'intégrité et la sécurité des données et des informations.

²⁴ En respectant par exemple un délai de préavis raisonnable.

²⁵ Voir notamment : art. 202, §1, 7° de la loi OPCVM ; art. 29, §1, 7° de la loi OPCA ; art. 75, al. 1, f) du Règlement AIFM ; art. 31, al. 2, c) du Règlement MiFID II.

En son sein, la SGPCI/SG peut confier le suivi effectif à un organe opérationnel ou, par exemple, désigner une personne de liaison. Les membres de l'organe en question ou la personne de liaison doivent disposer, par rapport aux tâches externalisées, de connaissances et d'expérience suffisantes pour leur permettre d'analyser d'un œil critique les prestations et les résultats du prestataire de services.

La FSMA souligne que les méthodes de suivi de la SGPCI/SG et les rapports de ses prestataires de services doivent être adaptés à la nature des fonctions externalisées et aux risques qui y sont liés. La SGPCI/SG prévoit à cet effet des canaux de communication clairs et impose au prestataire de services une obligation de déclaration de tout problème ayant ou pouvant avoir un impact sur les fonctions externalisées, ainsi que de toute situation d'urgence.

La SGPCI/SG procède régulièrement à une évaluation des prestataires de services, à l'aide d'outils tels que des indicateurs clés de performance, des indicateurs de contrôle clés, des rapports sur les prestations de services, l'auto-certification ou des examens indépendants et toute autre information pertinente reçue des prestataires de services.

Certains prestataires de services disposent d'une certification externe ou de rapport d'audit interne ou externe. Ces documents – s'ils peuvent être communiqués par le prestataire – peuvent être d'une aide précieuse lors des contrôles effectués par la SGPCI/SG. La FSMA attire cependant l'attention des SGPCI/SG sur le fait qu'il convient de se servir de tels rapports en connaissance de cause et avec circonspection. La SGPCI/SG ne devrait recourir à une telle méthode que si elle :

- est satisfaite du plan d'audit pour la fonction externalisée ;
- veille à ce que le périmètre de la certification ou du rapport d'audit couvre les systèmes (à savoir les processus, les applications, les infrastructures, les centres de données, etc.) et les contrôles considérés comme essentiels, ainsi que le respect des exigences réglementaires pertinentes ;
- évalue, de manière approfondie et continue, le contenu des certifications ou des rapports d'audit, et s'assure que les rapports ou les certifications ne sont pas obsolètes ;
- s'assure que les systèmes et contrôles essentiels sont couverts dans les futures versions de la certification ou du rapport d'audit ;
- est satisfaite de l'aptitude de la partie chargée de la certification ou de l'audit (notamment en ce qui concerne la rotation de l'entreprise chargée de la certification ou de l'audit, les qualifications, l'expertise, l'exécution/la vérification des éléments probants inclus dans le dossier d'audit sous-jacent) ;
- s'assure que les certifications sont délivrées et que les audits sont effectués sur la base de normes professionnelles pertinentes largement reconnues et qu'ils incluent un test relatif à l'efficacité opérationnelle des contrôles essentiels en place ;
- a le droit contractuel de demander l'extension du périmètre des certifications ou des rapports d'audit à d'autres systèmes et contrôles pertinents; le nombre et la fréquence de ces demandes de modification du périmètre devraient être raisonnables et légitimes du point de vue de la gestion des risques ;
- conserve le droit contractuel d'effectuer, à sa discrétion, des audits individuels en ce qui concerne l'externalisation de fonctions critiques ou importantes.

La SGPCI/SG doit prendre des mesures appropriées si elle constate des lacunes dans l'exercice de la fonction externalisée. En particulier, la SGPCI/SG devrait assurer le suivi de toute indication selon

laquelle les prestataires de services pourraient ne pas exercer la fonction critique ou importante externalisée d'une manière efficace ou conforme aux lois et aux exigences réglementaires applicables. Les mesures peuvent notamment comprendre la résiliation de l'accord d'externalisation avec effet immédiat, si nécessaire.

4.2.4 Stratégies de sortie²⁶

En cas d'externalisation de fonctions critiques ou importantes, la SGPCI/SG doit disposer d'une stratégie de sortie documentée qui soit conforme à sa politique d'externalisation ainsi qu'à son plan de continuité de l'activité, et qui prenne au moins en compte les éventualités suivantes :

- la résiliation des accords d'externalisation ;
- la défaillance du prestataire de services ;
- la détérioration de la qualité de la fonction assurée et les perturbations réelles ou potentielles de l'activité dues à la fourniture inadéquate ou défaillante de la fonction ;
- les risques significatifs découlant de la fourniture adéquate et continue de la fonction.

La SGPCI/SG doit veiller à être en mesure de se retirer des contrats d'externalisation sans que cela n'entraîne de perturbations dans ses activités commerciales, sans limiter sa conformité aux exigences réglementaires et sans nuire à la continuité et à la qualité des services qu'elle fournit aux clients. Pour ce faire, elle devrait :

- élaborer et mettre en œuvre des plans de sortie complets, documentés et suffisamment testés, le cas échéant (par ex., en effectuant une analyse des éventuels coûts, incidences, ressources et conséquences en termes de délais du transfert d'une fonction externalisée vers un autre prestataire) ;
- définir des solutions alternatives et élaborer des plans de transition pour lui permettre de retirer et de transférer des fonctions et des données externalisées du prestataire de services vers d'autres prestataires, ou de les internaliser, ou de prendre d'autres mesures garantissant la continuité de l'exercice de la fonction, d'une manière contrôlée et suffisamment testée, en tenant compte des difficultés susceptibles de résulter de la localisation des données et en prenant les mesures nécessaires au maintien de la continuité des activités pendant la phase de transition.

La SGPCI/SG s'attache en la matière aux points d'attention suivants :

- les technologies, systèmes et outils utilisés sont suffisamment répandus, connus et protégés contre les risques de cyberattaque et de fraude. Les solutions moins usuelles ou dépendant de manière excessive du prestataire de services sont à éviter ;
- le prestataire de services établit une bonne documentation fonctionnelle concernant ses systèmes et l'actualise régulièrement ;
- la SGPCI/SG dispose en interne de suffisamment de connaissances sur le fonctionnement, l'organisation et la gestion des fonctions externalisées ;
- les données propres peuvent être récupérées à tout moment dans un format utilisable ;

²⁶ Voir notamment : art. 75, al. 1, g) du Règlement AIFM ; art. 31, §2, l) du Règlement MiFID II.

- l'existence de procédures de notification et de réaction aux changements liés à un dispositif d'externalisation ou à un prestataire de services (tels que des changements liés à sa situation financière, à ses structures organisationnelles, à la sous-externalisation).

Lors de l'élaboration de stratégies de sortie, la SGPCI/SG devrait :

- définir les objectifs de la stratégie de sortie ;
- réaliser une analyse d'impact sur l'activité qui soit proportionnée au risque de la fonction externalisée, afin de déterminer les ressources humaines et financières nécessaires à la mise en œuvre du plan de sortie ainsi que le temps nécessaire pour procéder à la sortie du dispositif d'externalisation ;
- attribuer des fonctions, des responsabilités et des ressources suffisantes pour la gestion des plans de sortie et des activités de transition ;
- définir des critères de réussite de la transition des fonctions et des données externalisées ;
- définir les indicateurs à utiliser pour le suivi du dispositif d'externalisation (cf. section 4.2.3), y compris des indicateurs fondés sur des niveaux de service inacceptables qui devraient déclencher la sortie.

4.2.5 Notification à la FSMA en cas d'externalisation de fonctions critiques ou importantes²⁷

La FSMA rappelle que, sauf disposition légale contraire, aucune externalisation ne requiert en principe son accord préalable. Ceci ne porte pas préjudice au droit de la FSMA de contrôler si l'externalisation respecte la réglementation applicable. Dans ce cadre, la FSMA rappelle que les principes de saine gestion développés dans le présent guide pratique doivent être pris en considération.

Cependant, en cas d'externalisation de fonctions critiques ou importantes, la SGPCI/SG doit informer la FSMA au préalable de la manière dont les principes énoncés dans le présent guide pratique seront appliqués. La SGPCI/SG le fait savoir à la FSMA avant l'entrée en vigueur du contrat d'externalisation²⁸.

Ce même devoir d'information porte également sur toute évolution ultérieure importante concernant les fonctions critiques ou importantes externalisées.

5 Conclusion

Comme indiqué en introduction de ce guide pratique, l'externalisation peut, dans de bonnes conditions, contribuer à une meilleure gestion par le transfert de certaines fonctions à des tiers. La FSMA insiste sur le fait qu'elle ne diminue toutefois en rien la responsabilité de la société de tenir compte des principes de saine gestion dans la conduite de ses activités.

Chaque SGPCI/SG doit, dès lors, mener en permanence une politique appropriée en matière d'externalisation de fonctions, en vue du maintien d'une organisation adéquate visant à garantir une gestion saine et efficace de la société.

²⁷ Voir notamment : art 202, §1, 1° de la loi OPCVM et art. 29, §1, 1° de la loi OPCA.

²⁸ Une telle obligation est par ailleurs expressément prévue dans les cas visés à l'art. 29, §1^{er}, 1° de la loi OPCA et l'art. 202, §1^{er}, 1° de la loi OCPVM.

L'organisation adéquate, ainsi que son contrôle, constituant la pierre angulaire du contrôle prudentiel exercé par la FSMA, celle-ci attend, de la part de chaque SGPCI/SG qui recourt à l'externalisation, qu'elle le fasse en conformité avec la législation applicable et en prenant le présent guide pratique en considération.