DECEMBRE 2019

SYNTHÈSE DES CONTRÔLES SPOT 2019 DISPOSITIF DE CYBER SÉCURITÉ DES SOCIÉTÉS DE GESTION DE PORTEFEUILLE

amf-france.org

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

INTRODUCTION

Comme annoncé dans les priorités de supervision 2019 de l'AMF, la première série de contrôles SPOT de l'année 2019 visant des sociétés de gestion de portefeuille (« SGP ») a porté sur la revue des dispositifs de cyber sécurité de 5 acteurs : « *L'augmentation continue des menaces a accru la prise de conscience des enjeux liés à la cyber sécurité pour les acteurs des marchés financiers. L'AMF a mené fin 2018 de premiers travaux pour faire le bilan de l'organisation des SGP en matière de sécurité informatique […] Cette première collecte d'information […] sera complétée en 2019 par des contrôles SPOT et des contrôles classiques [visant l'] organisation, [les] procédures et [l']'effectivité du dispositif déployé pour assurer la gouvernance et la sécurité des Systèmes d'Information* ».

L'objectif principal de ces contrôles ciblés a été de s'assurer (i) de la prise en compte adéquate des risques cyber et (ii) de l'efficacité des contrôles mis en œuvre pour adresser ces risques. Le choix de ce thème a été motivé par la conjonction de nombreux facteurs de risques parmi lesquels la dépendance croissante de l'industrie aux outils dématérialisés et aux prestataires informatiques externes (par exemple : les services 'Cloud').

Ces contrôles sur le dispositif de cyber sécurité ont été réalisés conjointement dans cinq SGP. Les vérifications ont porté principalement sur la période 2016-2018[1] et ont permis d'examiner :

- ☐ l'organisation du dispositif de cyber sécurité des SGP contrôlées (ressources internes/externes, formation des collaborateurs) ;
- ☐ la gouvernance de ce dispositif (stratégie de la sécurité des Systèmes d'Information (« SSI »), cartographie des systèmes et des risques informatiques associés, corps procédural, comitologie) ;
- ☐ l'administration du Système d'Information (« SI ») (postes de travail, serveurs, réseau filaire, Wi-Fi, messagerie) ;
- ☐ le dispositif de surveillance du SI et notamment le processus de gestion des incidents informatiques (détection, analyse, résolution, revue post-mortem) ;
- ☐ la gestion des données sensibles (existence d'une politique de classification des données par niveau de criticité et d'une cartographie de ces données) ;
- ☐ le plan de continuité d'activité (existence d'un site de secours, d'un dispositif miroir, d'une stratégie de reprise d'activité informatique, revue du processus de sauvegarde régulière des données, prise en compte des risques cyber sur cette stratégie) ;
- ☐ les contrôles en place sur le SI (gestion des accès logiques, des changements et de l'exploitation informatique) et le dispositif de cyber sécurité.

Cette synthèse fait écho à l'enquête réalisée par la Direction de la gestion d'actifs de l'AMF en 2018 auprès de 40 SGP françaises. Elle a également utilisé (i) les constats de la mission de contrôle classique menée en 2019 sur le dispositif de cyber sécurité d'une SGP filiale d'une grande banque française, ainsi que (ii) les données de l'enquête[2] publiée par l'AFG en octobre 2018 sur le thème « *cyber sécurité : procédures et moyens mis en œuvre au sein des SGP* ».

---

1 Plusieurs pièces fournies (notamment des procédures ou des rapports d'audit de sécurité) sont datées de l'année 2019 mais couvrent le Système d'Information tel qu'existant en 2018.

2 Réalisée sur un échantillon de 70 SGP (dont 28 filiales de groupe financier et 42 SGP entrepreneuriales) gérant un encours de 4 Mds€ et employant près de 15 000 personnes.

Ces contrôles ont donné lieu à des lettres de suites comportant des demandes de remédiation aux points de non-conformité relevés. La présente synthèse a ainsi pour objet d'apporter un éclairage sur les pratiques des SGP sous revue sur le dispositif de contrôle cyber de leurs données sensibles, de leurs processus clés et de leur Systèmes d'Information en général.

Ce document, qui ne constitue ni une position, ni une recommandation, ne saurait introduire d'éléments de doctrine. Les pratiques identifiées comme 'bonnes' ou 'mauvaises' ne sont pas l'expression d'une doctrine de l'AMF. Elles soulignent des approches dominantes constatées lors des contrôles et susceptibles de favoriser, ou de compliquer[3], la gestion efficace et pérenne des risques de cyber sécurité et de leurs conséquences potentielles tant opérationnelles que réglementaires.

SOMMAIRE

[3] Une mauvaise pratique pouvant être à l'origine d'un manquement.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

1- PRINCIPALES NOTIONS ET GLOSSAIRE

➢ *Définition du risque de cyber sécurité*

Le risque de cyber sécurité découle de **toute atteinte malveillante potentielle, interne ou externe, à l'une des caractéristiques clés du Système d'Information d'une SGP** c'est-à-dire sa disponibilité, son intégrité, la confidentialité des données qu'il traite, la traçabilité de leurs actions et leur non-répudiation[4]. Il est usuel de résumer ces caractéristiques par l'acronyme **D.I.C.T. (Disponibilité, Intégrité, Confidentialité, Traçabilité)**. Ce risque peut cibler les placements collectifs et/ou mandats gérés : il s'assimile alors à un risque opérationnel mais ne s'y réduit pas. Sa réalisation peut en effet également conduire à une non-conformité réglementaire[5] de la SGP dans les domaines relatifs à l'existence et au maintien :

- ☐ du **niveau de fonds propres réglementaires** (ces derniers pouvant être obérés en cas de rupture d'activité) ;
- ☐ d'une **politique rigoureuse de conservation et de maintien des données opérationnelles**, notamment aux fins de contrôles par l'AMF (sur les transactions opérées et la lutte anti-blanchiment) ;
- ☐ d'un **plan de continuité d'activité** (PCA) adapté, testé et efficace (une attaque cyber pouvant rendre inutilisables les infrastructures informatiques de la SGP et/ou les installations de secours et/ou les sauvegardes effectuées) ;
- ☐ de **moyens (informatiques) adaptés et suffisants** ;
- ☐ d'un **dispositif solide de protection des données sensibles** (relatives aux investisseurs, aux fonds et aux mandats).

Les analyses de la mission de contrôle sur les processus de gestion des données sensibles n'ont pas porté sur la vérification de conformité à la réglementation RGPD. Il est toutefois rappelé que le risque de cyber sécurité peut avoir un impact sur le respect, par la SGP, de ses obligations liées au RGPD lorsqu'il affecte des données à caractère personnel.

Il est par ailleurs précisé 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 (gestion d'OPCVM) et 318-6 (gestion de FIA) du règlement général de l'AMF).

➢ *Glossaire*

terme	définition
« *Active directory* »	Service d'annuaire fourni par Microsoft. Il a pour objectif de centraliser l'identification et l'authentification d'un réseau de postes et serveurs Windows, ce qui permet la gestion centralisée par les administrateurs de la configuration des socles, des droits utilisateurs, de l'installation des logiciels et des mises à jour.
Authentification forte	Procédure d'authentification qui requiert la concaténation d'au moins deux facteurs d'authentification à savoir ce que l'utilisateur connaît (par exemple un mot de passe) et ce qu'il détient (à savoir par exemple un jeton d'authentification).
CERT	« *Computer Emergency Response Team* » : centre d'alertes et de réactions aux attaques informatiques[6]

[4] Capacité du Système d'Informations (SI) à associer de manière univoque (et sans contestation possible) les actions réalisées dans le SI par un utilisateur au compte informatique de ce même utilisateur. Cette fonctionnalité est essentielle pour établir avec certitude une piste d'audit des actions menées dans le SI.

[5] Se référer à l'encadré « principales règles de droit » ci-dessous.

[6] L'ANSSI précise le rôle de ces équipes sur son site Internet : https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/

terme	définition
« *cloud* »	Utilisation de serveurs informatiques distants (du site de la société utilisatrice), par l'intermédiaire d'un réseau informatique, dans le but d'y stocker des données ou de les exploiter.
« *hacking* »	Piratage informatique
miroir	Dispositif technique de continuité d'activité permettant la réplication en temps réel des données d'un serveur vers un autre serveur situé à distance. En cas de faille sur le serveur principal, le Système d'Information peut redémarrer rapidement grâce à l'usage du serveur miroir, avec un risque de perte de données minime voir nul.
« *phishing* »	Technique utilisée par les fraudeurs pour obtenir des renseignements personnels dans le but d'usurper l'identité d'un individu ou d'une organisation.
« *proxy* »	Composant informatique jouant le rôle d'intermédiaire entre le réseau mondial Internet et le réseau informatique de la SGP afin de faciliter et surveiller les échanges.
SOC	« *Security Operations Center* » : système de surveillance centralisé des activités anormales du SI
Wi-Fi	« *Wireless Fidelity*» : réseau local permettant de relier sans fil plusieurs appareils informatiques

Note liminaire :
Les bonnes et mauvaises pratiques identifiées en cours de contrôle (et mentionnées ci-dessous) sont à considérer à l'aune de l'échantillon de SGP contrôlées à savoir, pour 4 sociétés sur 6, des filiales de Groupes de grande taille dotés d'importants moyens.

2- RÉSUMÉ DES PRINCIPAUX ENSEIGNEMENTS DE LA MISSION

Les travaux ont permis de constater que l'ensemble des SGP contrôlées ont pris la mesure du risque cyber en l'intégrant dans leur cartographie, en collectant les incidents de cyber sécurité qu'elles subissent et en faisant appel à des prestataires spécialisés pour vérification de la robustesse de leur SI. Ces dispositifs assurent une couverture technique raisonnable des principaux risques cyber, aux exceptions près détaillées ci-après.

En revanche, ils ne prennent pas en compte les impacts potentiels de la matérialisation des risques de cyber sécurité sur la conformité réglementaire des SGP en matière de (i) niveau de fonds propres, (ii) de conservation des données et (iii) de plan de continuité d'activité et de moyens (informatiques). La majorité des SGP contrôlées (4/6) bornent en effet le risque cyber au seul risque opérationnel (impact sur les investisseurs).

Par ailleurs, la mission de contrôle a constaté l'absence fréquente de cartographies exhaustives (i) des données sensibles et (ii) des systèmes critiques, ainsi que d'une politique de classification des données, premières briques pourtant essentielles d'une approche cyber pérenne permettant la priorisation pertinente des actions de sécurité.

De surcroît, l'identification formelle des incidents cyber, pour l'évaluation continue du niveau de risque associé, s'avère malaisée. Les incidents de cyber sécurité avérés (i.e. ayant eu un impact sur le SI) sont en effet fréquemment confondus, dans les bases de collecte, avec des attaques externes ayant été bloquées avec succès par le dispositif de contrôle et/ou avec des incidents informatiques internes basiques et non intentionnels (exemple : panne serveur).

D'autre part, pour les SGP appartenant à un groupe (5/6 dont 4 appartenant à des groupes de grande taille), il a été identifié un pilotage insuffisant des prestations (relatives à l'informatique, la cyber sécurité et la continuité d'activité) rendues par la maison-mère. D'un côté, ces prestations globales permettent aux SGP filiales de bénéficier de l'expertise et des moyens du groupe. Toutefois, elles s'appuient sur le modèle générique de la maison-mère bancaire, sans prise en compte suffisante des spécifités métier et réglementaires de la filiale SGP.

Cette porosité SGP/Groupe génère des situations risquées du point de vue technique (par exemple : l'imbrication du réseau informatique de la SGP dans celui du groupe, exposant directement la première en cas d'attaque du second) et organisationnel (par exemple : le manque de visibilité de la SGP sur le caractère exhaustif et efficace des services rendus par le groupe tels que la sauvegarde des données et les tests d'intrusion). Elle conduit par ailleurs les SGP concernées à s'exonérer du pilotage direct de leurs risques cyber, arguant du manque d'expertise en interne par rapport aux moyens du groupe. Or, le travail principal et prioritaire de protection contre les risques

cyber relève de la responsabilité de la SGP. De plus, ce travail étant, en pratique, d'ordre organisationnel et procédural, il peut être entrepris par des sociétés de taille réduite. Le travail technique, certes réel, n'arrive qu'en second lieu et peut être en effet, une fois le précédent réalisé, délégué à des tiers spécialisés.

3- CONTEXTE ET PÉRIMÈTRE

3.1- INTRODUCTION

En France, la notion de cybercriminalité a été définie initialement dans la loi informatique et libertés de 1978. Cette notion a été précisée par la suite dans plusieurs lois successives entre 1988 (loi Godfrain sur la fraude informatique) et 2006 (loi anti-terrorisme). Dans ce cadre, la France a créé en 2009, au sein du Secrétariat général de la défense et de la sécurité nationale, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

L'AMF participe à la réflexion sur les risques de cyber sécurité au travers de plusieurs groupes de travail internationaux (en liaison avec la Banque de France et le Trésor) tels que le « *Cyber Expert Group* » (CEG) du G7, le « *Financial Stability Board* » (FSB) et l' « *European Systemic Cyber Group* » (ESCG) de l'ESRB (« *European Systemic Risk Board* »).

À l'échelle européenne, **les autorités de surveillance** (« ESAs »[7]) **ont émis, en février 2019, un avis conjoint relatif à la cyber sécurité (valant proposition législative)**[8]. Cet avis mentionne la nécessité d'**une plus grande harmonisation** des règles (i) de gouvernance locales de la cyber sécurité et (ii) **d'identification, de collecte et de reporting des incidents cyber aux régulateurs**. Il évoque également le besoin d'une grille de contrôle commune aux membres portant sur **la surveillance des prestataires informatiques critiques, notamment ceux fournissant des services de « *cloud computing* »**[9]. Il suggère enfin la mise en place progressive d'un cadre cohérent et proportionné de **tests techniques de la cyber résilience des établissements régulés**, via la réalisation de tests d'intrusion.

3.2- PRÉSENTATION DE L'ÉCHANTILLON DE SGP CONTRÔLÉES

Les SGP retenues pour ces contrôles thématiques ont été sélectionnées afin de constituer un panel des pratiques de place concernant les dispositifs de cyber sécurité dans la gestion d'actifs :

- ☐ la SGP n°1 est la filiale d'un groupe bancaire français. Elle est spécialisée dans le capital-investissement et gère des FPCI et des FPS ;
- ☐ la SGP n°2 est la filiale d'une SGP française. Elle est spécialisée dans la gestion des fonds monétaires ;
- ☐ la SGP n°3 est la filiale d'une banque américaine. Elle est spécialisée dans la gestion passive ;
- ☐ la SGP n°4 est la filiale d'un groupe financier français. À la différence des trois précédentes, elle est principalement orientée sur une clientèle non-professionnelle ;
- ☐ la SGP n°5 est une société entrepreneuriale.

L'AMF a également contrôlé en 2019, en parallèle des missions SPOT, une autre SGP filiale d'une banque française sur le thème de la cyber sécurité. Les résultats de ce contrôle 'classique' ont été intégrés dans les sections ci-

---

7 Les « ESAs » (« European Supervisory Authorities ») sont constituées de l'ESMA (« European Securities and Markets Authority », régulateur européen des marchés financiers), de l'EBA (« European Banking Authority », régulateur bancaire européen) et de l'EIOPA (« European Insurance and Occupational Pensions Authority », régulateur européen des assurances).

8 Cet avis est accessible via : https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

9 Se référer à la définition du glossaire en début de synthèse.

dessous aux fins de comparaison avec l'échantillon de SGP contrôlées dans le cadre de la mission SPOT. La SGP en question porte le n°6.

Les investigations ont porté sur la période allant du 1er janvier 2016 au 31 décembre 2018.

3.3- RÉGLEMENTATION APPLICABLE

Pour réaliser ses travaux, la mission de contrôle s'est appuyée sur :

- ☐ le règlement général de l'AMF ;
- ☐ le code monétaire et financier ;
- ☐ le règlement délégué (UE) n°231/2013 de la directive AIFM ;
- ☐ le règlement délégué (UE) n°2017/565 de la directive MIF 2.

Principales sources de droit

Règles d'organisation

a) Article 321-23 (I)(II)(IV)(VI) du règlement général de l'AMF (OPCVM), article 318-1 du règlement général de l'AMF, article 57 (1) du règlement délégué (UE) n° 231/2013 (FIA) et article 21 (1) du règlement délégué (UE) n°2017/565 (gestion sous mandat – « GSM ») concernant **les moyens matériels, financiers et humains adaptés et suffisants dont la SGP doit se doter ;**

b) Article 321-23 (III)(V) du règlement général de l'AMF (OPCVM), articles 22 et 57 (1 b) du règlement délégué (UE) n° 231/2013 (FIA) et article 21 (1)(b)(d) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'emploi par les SGP de personnels disposant des compétences, des connaissances et de l'expertise requises ;**

c) Articles 321-83 du règlement général de l'AMF (OPCVM), article 62 du règlement délégué (UE) n° 231/2013 (FIA) et article 24 du règlement délégué (UE) n°2017/565 (GSM) concernant **l'établissement et le maintien d'une fonction de contrôle périodique exercée de manière indépendante ;**

d) Article 321-25 du règlement général de l'AMF (OPCVM), article 57 (3) du règlement délégué (UE) n° 231/2013 (FIA) et article 21 (3) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'établissement et le maintien d'un plan de continuité d'activité garantissant, en cas d'interruption des systèmes et procédures, la sauvegarde des données essentielles et la poursuite des activités de gestion ;**

Dispositif de conformité

e) Article 321-30 du règlement général de l'AMF (OPCVM), articles 318-4 du règlement général de l'AMF et 61 (1) du règlement délégué (UE) n° 231/2013 (FIA), articles 312-1 du règlement général de l'AMF et 22 (1) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'établissement et le maintien opérationnel de politiques, procédures et mesures adéquates permettant la détection de tout risque de non-conformité ;**

f) Article 321-31 du règlement général de l'AMF (OPCVM), article 61 (2) du règlement délégué (UE) n° 231/2013 (FIA) et article 22 (2) du règlement délégué (UE) n°2017/565 (GSM) concernant **la mise en place d'une fonction de conformité efficace exercée de manière indépendante ;**

Responsabilité des dirigeants

g) Article 321-35 (g) du règlement général de l'AMF (gestion d'OPCVM), articles 318-6 du règlement général de l'AMF et 13 (2) du règlement délégué (UE) n° 231/2013 (gestion de FIA) concernant **la collecte des incidents et l'information associée des dirigeants et de l'AMF** ;

h) Article 321-36 du règlement général de l'AMF (OPCVM), article 60 (4) du règlement délégué (UE) n° 231/2013 (FIA) et article 25 (2) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'information régulière des dirigeants quant aux résultats des contrôles permanents et périodiques ;**

Gestion des risques

j) Article 321-77 du règlement général de l'AMF (OPCVM), articles 38 et 39 du règlement délégué (UE) n° 231/2013 (FIA) et article 23 du règlement délégué (UE) n°2017/565 (GSM) concernant **la mise en place d'une fonction de gestion des risques exercée de manière indépendante ;**

i) Articles 321-78 et 321-79 du règlement général de l'AMF (OPCVM), article 40 du règlement délégué (UE) n° 231/2013 (FIA) et articles 312-46 du règlement général de l'AMF et 23 du règlement délégué (UE) n°2017/565 (GSM) concernant l'établissement **et le maintien opérationnel d'une politique de gestion des risques appropriée et documentée qui permet de déterminer les risques auxquels les placements collectifs ou les portefeuilles individuels sont ou pourraient être exposés ;**

k) Articles 321-35 et 321-80 du règlement général de l'AMF (OPCVM), articles 41 et 60 (2) du règlement délégué (UE) n° 231/2013 (FIA), article 312-47 du règlement général de l'AMF et article 25.1 du règlement délégué (UE) n° 2017/565 (GSM) concernant **le contrôle régulier des politiques et procédures de gestion des risques ;**

l) Article 321-81 du règlement général de l'AMF (OPCVM), article 39 du règlement délégué (UE) n°231/2013 (FIA) et article 312-48 du RG AMF (GSM) concernant la **mesure et la gestion à tout moment des risques auxquels les placements collectifs ou les portefeuilles individuels sont exposés ou susceptibles d'être exposés ;**

m.1) Article 321-76 du règlement général de l'AMF (OPCVM), article 13 du règlement délégué (UE) n° 231/2013 (FIA) et article 312-44 du règlement général de l'AMF (GSM) concernant la **définition du risque opérationnel de perte pour le placement collectif ou le portefeuille individuel ;**

m.2) Article 13 du règlement délégué (UE) n° 231/2013 (FIA) concernant la **définition du risque opérationnel pour la SGP AIFM ;**

Externalisation

n) Articles 321-93 à321-96 du règlement général de l'AMF (OPCVM), articles 318-58 à 318-61 du règlement général de l'AMF (FIA), article L.533-10 II 4°du code monétaire et financier et article 30 (1) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'externalisation des prestations de services essentiels ;**

Enregistrement et conservation des données

o) Article 321-24 du règlement général de l'AMF (OPCVM), article 57 (2) du règlement délégué (UE) n° 231/2013 (FIA) et article 21 (2) du règlement délégué (UE) n°2017/565 (GSM) concernant **l'obligation de sauvegarde de la sécurité, l'intégrité et la confidentialité des informations traitées par la SGP ;**

p) Articles L. 533-8 et L. 533-10 II 6° du code monétaire et financier relatifs à l'**obligation de conservation des informations pertinentes associées aux transactions effectuées ;**

q) Articles 321-69 à 321-74 du règlement général de l'AMF (OPCVM), articles 57 (1), 58 et 64 à 66 du règlement délégué (UE) n°231/2013 (FIA) et article 312-41 du règlement général de l'AMF et article 75 du règlement délégué (UE) n°2017/565 (GSM) relatifs à **l'enregistrement et à la conservation des données nécessaires au contrôle des opérations réalisées par la SGP.**

4- CONSTATS ET ANALYSES

Dans l'approche des contrôles SPOT, trois types de constats peuvent être émis : les manquements (comme pour les contrôles 'classiques') et les bonnes ou mauvaises pratiques.

Le **manquement à la réglementation** traduit le non-respect identifié d'un texte précis de la réglementation (qui sera cité dans la synthèse).

Les bonnes ou mauvaises pratiques ont été définies en introduction du présent document.

4.1- ORGANISATION DU DISPOSITIF DE CYBER SÉCURITÉ ET MOYENS MIS EN ŒUVRE

➢ *Indépendance de la fonction cyber sécurité*

Le Système d'Information (« SI ») des cinq SGP de l'échantillon contrôlé appartenant à un groupe (n°1, 2, 3, 4, 6) est inclus dans le SI de ce dernier. Ainsi, c'est le groupe qui est en charge de la maintenance, de l'évolution et de la surveillance du SI de la SGP. La SGP n°3 est la seule à présenter une situation légèrement différente dans la mesure où elle utilise une application de gestion externe (fournie par un éditeur français) qui n'est pas un standard du Groupe.

Dans ce cadre, **le SI de quatre de ces cinq SGP est piloté par le DSI Groupe et contrôlé par le responsable de la sécurité des Systèmes d'Information (« RSSI ») Groupe** (le recrutement d'un RSSI interne est en cours chez la SGP n°4). Cette dépendance au groupe se double d'une dépendance importante aux prestataires externes pour les SGP n°1, 3 et 4, principalement due aux applications métier utilisées par ces SGP. La SGP n°6, à l'inverse, dispose de ses propres DSI et RSSI.

Pour les SGP n°1, 2, 3 et 6, **l'indépendance de la fonction RSSI par rapport au DSI** est assurée :

- Par un rattachement hiérarchique ou fonctionnel du RSSI Groupe au comité exécutif (pour les SGP n°2 et 3 et 6) ;
- Par l'existence d'une fonction de contrôle indépendante (rattachée à la direction de la conformité) de la RSSI (pour la SGP n°1).

La SGP n°5, seule SGP indépendante, ne dispose ni d'une DSI ni d'un RSSI. Elle est intégralement dépendante d'un prestataire informatique externe unique (présent depuis la création de la SGP), pour la maintenance, les évolutions et la cyber surveillance de son SI. Ce prestataire réalise cette mission sous la supervision du PDG de la SGP.

➢ *Budget du dispositif de cyber sécurité par rapport au budget de la DSI*

Le suivi du ratio « budget dévolu à la cyber sécurité / budget de la fonction informatique » constitue un indicateur de pilotage du dispositif de cyber sécurité utile au management de la SGP. Il permet en effet de mesurer l'évolution de la prise en compte du risque cyber (par la réalisation de tests d'intrusion externalisés par exemple) dans les dépenses informatiques globales (qui couvrent par exemple le remplacement des serveurs).

La mission de contrôle note dans ce cadre que les dépenses informatiques sont correctement identifiées pour l'ensemble des SGP contrôlées. Les SGP n°1, 2 et 4 ont été par ailleurs en mesure de fournir le ratio « budget cyber / budget DSI » calculé au niveau de leur Groupe d'appartenance (il est compris entre 1 et 3 %). La SGP n°6 a quant à elle pu fournir ce ratio (calculé à son propre niveau) : le budget cyber de cette SGP représente en 2018 6 % du budget de sa DSI.

➢ *Sensibilisation des équipes aux risques de cyber sécurité*

Des programmes de sensibilisation des salariés n'ont été mis en place que dans les 4 SGP de l'échantillon présentant les actifs sous gestion les plus importants (i.e. les SGP n°1, 2, 3 et 6).

Toutefois, pour les SGP n°1 et 2, ces programmes n'incluent pas de tests de « *phishing* ». Les SGP n°3 et 6, qui ont mis en place ce type de tests, disposent d'un outil de pilotage efficace de l'évolution du niveau de vigilance des collaborateurs (ce qui leur permet notamment de renforcer les formations sur les populations dont les résultats aux tests montrent qu'elles le nécessitent).

Au sein de la SGP n°6, aucun suivi consolidé global ne permet de mesurer l'évolution du niveau de prise de conscience du risque de cyber sécurité par les utilisateurs du SI.

Rappel réglementaire :

- La SGP s'assure que les personnes concernées sont bien au courant des procédures qui doivent être suivies en vue de l'exercice approprié de leurs responsabilités. Elle emploie un personnel disposant des qualifications, des connaissances et de l'expertise requises pour exercer les responsabilités qui lui sont confiées » Article 321-23 III et V du RG AMF (OPCVM), articles 22 et 57(1b) du règlement délégué (UE) n° 231/2013 (FIA), article 21 1) b) et d) du règlement délégué n°2017/565 (GSM).

Bonnes pratiques :

- Assurer l'indépendance de la fonction RSSI par rapport à la DSI soit par un rattachement (hiérarchique ou fonctionnel) du RSSI au comité exécutif, soit par l'instauration d'une fonction de contrôle indépendante des activités du RSSI.
- Sensibiliser les collaborateurs de la SGP aux risques de cyber sécurité en les intégrant au plan de formation annuel et réaliser, au moins annuellement, un test de « *phishing* » (structuré différemment d'une année sur l'autre) sur l'ensemble des collaborateurs de la SGP afin de vérifier l'évolution de leur niveau de sensibilité aux risques cyber.
- Isoler, dans les dépenses informatiques annuelles de la SGP, celles liées à la cyber sécurité.

4.2- GOUVERNANCE DU DISPOSITIF DE CYBER SECURITÉ

➢ *Stratégie de cyber sécurité*

Les SGP n°2, 3, 5 et 6 articulent leur dispositif de cyber sécurité autour d'une stratégie claire et formalisée, validée par le comité exécutif du groupe (pour les SGP n°2, 3 et 6) ou de la SGP n°5**.** Cette approche présente l'avantage de fournir un cadre formel pérenne aux travaux de cyber sécurité, de les prioriser en fonction de risques préalablement définis comme prioritaires et de les rendre accessibles aux non-spécialistes (internes comme externes).

Les SGP n°2, 3 et 6 appliquent la stratégie de leur groupe d'appartenance. La SGP n°5 (qui est indépendante) a défini sa propre stratégie, en ligne avec ses moyens limités et ses principaux risques. Celle-ci s'appuie sur :

- le maintien d'un parc matériel et logiciel à jour et homogène ;
- la ségrégation des accès logiques aux données et opérations sensibles ;
- une analyse anticipative du risque de rupture d'activité.

À l'opposé, les **SGP n°1 et 4 n'ont pas défini de stratégie de cyber sécurité.**

Les stratégies de cyber sécurité des SGP contrôlées s'appuient sur les référentiels de place présentés ci-dessous. La mission de contrôle a constaté que les référentiels les plus utilisés étaient le guide d'hygiène de l'ANSSI ainsi que le référentiel NIST[10] (notamment par la SGP n°6).

Nom	Emetteur	Lien
Le guide d'hygiène	ANSSI	https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
Guide de la sécurité des données personnelles	CNIL	https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles
« *Cybersecurity framework* »	NIST « *National institute of standards and technology* »	https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[10] « *National Institute of Standards and Technology* » : organe du « *US department of Commerce* » ayant développé un référentiel international de cyber sécurité.

Nom	Emetteur	Lien
Normes 27001 et 27002	ISO/IEC « *International Organization for Standardization/International Electrotechnical Commission* »	https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
« *fundamental elements for cyber security in the financial sector* »	G7	https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf
COBIT 5 « *control objectives for information and related technology* »	ISACA « *information system audit and control association* »	https://www.isaca.org/cobit
CIS20 (liste de 20 contrôles de cyber sécurité décomposés en 6 'standards', 10 'fondamentaux' et 4 'organisationnels')	CIS « *Center for Internet Security* »	https://www.cisecurity.org/controls/cis-controls-list/

La mission de contrôle constate toutefois que la stratégie cyber Groupe est appliquée directement par les SGP n°2, 3 et 6 **sans marge d'adaptation claire quant à la prise en compte de leurs spécificités réglementaires et opérationnelles**. À titre d'exemple, la mission de contrôle n'a pas identifié dans les documents fournis (supports de comités ou fiches d'analyse des risques) de preuve de l'existence de telles adaptations. Or, la maison-mère respective de chacune de ces SGP étant une banque, il existe ici un risque d'inadéquation des mesures de sécurité prises aux enjeux réels des trois sociétés concernées. Ce risque est d'ailleurs d'autant plus notable que les prestations de cyber sécurité rendues par le groupe ne font pas l'objet d'un contrôle suffisant par ces SGP (se référer à la section 4.7 de la présente synthèse).

- ***Pilotage du risque cyber par les instances de direction des SGP***

Les risques de cyber sécurité bénéficient dans l'ensemble des SGP contrôlées d'un pilotage adéquat par les instances dirigeantes. Les 6 SGP contrôlées ont en effet désigné au sein de leur comité exécutif respectif un représentant en charge de ces risques. Il s'agit :

- du président de la SGP pour les SGP n°3 et 5 ;
- du secrétaire général pour les SGP n°2 et 4
- du directeur général adjoint en charge des finances pour la SGP n°1 ;
- d'un directeur général délégué pour la SGP n°6.

Par ailleurs, les SGP n°1, 2 et 6 ont renforcé leur pilotage de ces risques via leur intégration dans des comités dédiés.

- ***Outils de pilotage du risque de cyber sécurité***

Ces outils sont incomplets pour l'ensemble de l'échantillon contrôlé (sauf pour la SGP n°6 qui applique les procédures de son groupe d'appartenance), qu'il s'agisse de la cartographie des risques ou du corpus procédural (seule la SGP n°2 dispose, via les procédures de son groupe d'origine, d'un corpus couvrant à la fois l'identification des risques cyber, les contrôles en place, l'administration du SI, la gestion des incidents et le PCA).

Concernant la cartographie, seules les SGP n°1 et 6 ont réalisé un exercice exhaustif :

- En prenant en compte dans leur analyse les impacts potentiels des risques cyber en termes de non-conformité de la SGP (i) à la déclaration de moyens du programme d'activité, (ii) au niveau de fonds propres réglementaires requis, (iii) à la conservation, à l'intégrité et à la confidentialité des données sensibles (relatives aux investisseurs, aux instruments et aux transactions notamment) et (iv) au maintien opérationnel d'un PCA robuste ;

- En analysant également ces impacts en termes de pertes financières et de dégâts d'images (cette dernière analyse s'avérant particulièrement poussée pour la SGP n°6) ;

Les cinq autres SGP ont dans leur cartographie respective une approche réductrice du risque cyber en le cantonnant au seul risque opérationnel, sans connexion avec les nombreux manquements à la réglementation que la matérialisation d'un tel risque peut engendrer.

Concernant le corpus procédural sur la cyber sécurité, il ne s'avère complet que pour les SGP n°2 et 3 (au niveau Groupe). En effet :

- la SGP n°1 ne dispose pas de procédures à jour relativement à l'administration de son matériel informatique fixe/mobile et de son réseau Wi-Fi ;
- la SGP n°4 n'a pas mis en place de procédure de gestion des cyber incidents ;
- la SGP n°5 n'aborde le risque cyber dans son corpus que sous l'angle (réducteur) de la rupture d'activité.

Ces lacunes impliquent un risque de couverture insuffisante des risques de cyber sécurité pouvant avoir un impact sur les SGP contrôlées.

Rappel réglementaire :

↗ Les SGP établissent, mettent en œuvre et gardent opérationnelles des politiques et des procédures conçues pour détecter tout risque de manquement à leurs obligations professionnelles et mettent en place des mesures ou procédures pour minimiser ces risques - Article 321-30 du règlement général de l'AMF (OPCVM), articles 318-4 du règlement général de l'AMF et 61 (1) du règlement délégué (UE) n° 231/2013 (FIA), articles 312-1 du règlement général de l'AMF et 22 (1) du règlement délégué (UE) n°2017/565 (GSM)

Mauvaises pratiques :

↗ Pour les SGP filiales de groupes, n'appuyer leur dispositif de cyber sécurité que sur la stratégie groupe sans conserver de marges de négociation suffisantes pour adapter cette stratégie aux spécificités métier et règlementaires de la gestion d'actifs.

↗ Cantonner, dans la cartographie des risques des SGP, l'analyse des risques de cyber sécurité aux seuls impacts de risque opérationnel sur les fonds et/ou mandats gérés.

4.3- ADMINISTRATION DU SYSTÈME D'INFORMATION

➢ ***Cloisonnement du réseau***

La mission de contrôle note que les 5 SGP appartenant à un groupe (SGP n°1, 2, 3, 4 et 6) sont intégrées à son réseau informatique. Cette configuration va jusqu'à l'intégration complète de leur « *Active Directory* » (AD) dans celui du groupe, ce qui – à moyens de protections équivalents - est susceptible d'accroître l'exposition des SGP concernées au risque cyber en cas de sécurisation insuffisante de l'AD par le groupe[11].

Par ailleurs, la mission de contrôle a identifié (notamment sur la SGP n°4) une zone de risque potentielle dans l'intégration, sur une même infrastructure informatique, de plusieurs sociétés d'un même groupe exerçant des activités différentes (par exemple : SGP – activité n°1 – et banque d'affaires – activité n°2). Or, **en cas de gestion inefficace – au niveau groupe – des droits d'accès logiques au SI commun**, une telle intégration est susceptible de favoriser des accès non autorisés par les utilisateurs de l'activité 1 aux données sensibles de l'activité 2, en infraction à la « muraille de Chine » devant dissocier ces deux activités.

[11] L'« *active directory* » (AD) est défini dans le glossaire en début de synthèse.

➢ ***Processus d'administration du SI***

Les SGP n°1, 2, 4 et 5 présentent plusieurs vulnérabilités importantes et partagées aussi bien sur les postes de travail fixes et nomades que sur le réseau. Ces vulnérabilités (qui ont été identifiées par les SGP elles-mêmes) sont synthétisées ci-dessous.

Vulnérabilités identifiées	Risques induits	SGP N°1	SGP N°2	SGP n°4	SGP n°5
Procédures d'**administration du SI** absentes ou incomplètes	SI non homogène (du point de vue des versions d'applications ou d'antivirus par exemple) ce qui peut faciliter la création de points d'entrée pour un attaquant externe	X			
Inventaires des matériels fixes ou nomades **absents ou incomplets**			X		
Ports USB non bloqués sur les postes de travail fixes	Vol de données et/ou injection dans le SI d'un virus contenu dans une clé USB	X		X	X
Absence de proxy[12] dans le cadre des connexions à Internet des collaborateurs de la SGP	Téléchargement (non-détectable) de fichiers infectés sur des sites internet dangereux par les collaborateurs			X	X
Processus de **connexion distante** au SI insuffisamment sécurisé et contrôlé (pas d'authentification forte, protocoles faiblement sécurisés)	Accès au SI de la SGP par un attaquant externe se faisant passer pour un utilisateur interne	X		X	

Les éléments communiqués par SGP n°3 et 6 ont fourni à la mission de contrôle l'assurance raisonnable qu'elles ne présentaient pas les vulnérabilités identifiées dans le tableau ci-dessus.

Bonnes pratiques :

- ↗ Mettre en place des procédures d'administration du SI pour l'ensemble des équipements utilisés (matériel et réseau).
- ↗ Formaliser et mettre à jour régulièrement un inventaire des équipements informatiques utilisés.
- ↗ Mettre en place un contrôle des connexions des collaborateurs internes à Internet (incluant la traçabilité des navigations) ainsi qu'un contrôle des connexions distantes au SI.

Mauvaise pratique :

- ↗ Ne pas assurer le blocage des ports USB des postes utilisateurs.

4.4- SURVEILLANCE DU SYSTÈME D'INFORMATION

Les six SGP contrôlées ont défini et mis en place un processus de surveillance de leur système d'information. À titre d'exemple, les SGP n°2, 3, 5 et 6 bénéficient d'une plage de surveillance large (24 h/24 7j/7) de leur SI (au

[12] Se référer à la définition dans le glossaire en début de synthèse.

travers du « SOC[13] » Groupe pour les SGP n°2, 3 et 6, via le prestataire externe informatique pour la SGP n°5). En revanche, ce processus ne s'avère satisfaisant que pour 3 des 6 SGP contrôlées (les SGP n°2, 5 et 6). En effet :

- **concernant les SGP n°1 et 4, la surveillance du SI n'est active que pour les jours ouvrés, sur la période 7h – 19h** (sauf, pour la SGP N°1, sur les matériels utilisés par les dirigeants de la SGP). Cela induit un risque de réaction tardive en cas d'attaque cyber survenant hors des heures de travail, au risque de dégâts irrémédiables sur le SI ciblé ;
- **concernant la SGP n°3, elle ne reçoit aucune information quant aux résultats des opérations de surveillance menées sur son SI par le Groupe** (menaces détectées, attaques contrées, etc.).

➢ ***Processus de gestion des incidents cyber***

Les six SGP contrôlées ont également défini et mis en place un processus de gestion des incidents[14] de cyber sécurité. Ce processus s'avère robuste pour les SGP n°2, 5 et 6. Pour les trois autres SGP contrôlées :

- **concernant la SGP n°1, les incidents cyber ne sont pas identifiables aisément dans la base de collecte de l'ensemble des incidents en l'absence d'une clé d'identification unique** ;
- **concernant la SGP n°3, elle ne reçoit aucune information quant au traitement des incidents cyber ayant ciblé le SI Groupe.** Cela handicape la compréhension que la SGP pourrait avoir des menaces cyber pesant sur son activité et gêne donc sa capacité à pouvoir s'en prémunir **;**
- **concernant la SGP n°4, elle n'a pas mis en place de base répertoriant les incidents cyber** qu'elle a subis et traités.

L'analyse du volume d'incidents cyber remontés par chacune des SGP contrôlées fait apparaître une maîtrise encore imparfaite du processus de collecte des incidents cyber. En effet :

- **les SGP n°1 et 2, bien que gérant des volumes d'encours proches** (27,2 et 25,2 Mds€) et appartenant toutes deux à un groupe, **déclarent respectivement 502 et 4 incidents** sur la période couverte par le contrôle. Cette différence s'explique par la collecte pour la SGP n°1 des incidents cyber avérés et des attaques ayant été bloquées par le dispositif de cyber sécurité alors que la SGP n°2 ne collecte que les incidents avérés ;
- **la SGP n°3, sur la même période, indique n'avoir connu aucun incident cyber**, justifiant cela en indiquant qu'elle ne dispose pas de site Internet et n'a pas de contact direct avec la clientèle ;
- la SGP n°5 fait mention de 89 incidents cyber survenus sur son SI en 2018 mais l'analyse de ces derniers **montre qu'il s'agit plutôt d'opérations classiques de maintenance du SI** (par exemple : le changement d'un serveur ou la mise à jour d'un antivirus) ;
- quant à la SGP n°6, elle **cumule jusqu'à trois bases déclaratives différentes** dans lesquelles des incidents de cyber sécurité peuvent être renseignés. Ces trois bases visent respectivement (i) les suspicions de fuites de données, (ii) les incidents cyber touchant la SGP et (iii) ceux qui touchent le groupe. Toutefois, il n'existe pas de clé de lecture unique permettant de consolider simplement les données de ces bases, ce qui nuit à la visibilité sur l'évolution du niveau de risque cyber.

Note n°1 : Les carences identifiées *supra* dans la collecte des incidents cyber sont susceptibles de nuire à l'exhaustivité de la cartographie des risques cyber (dans la mesure où cette dernière se nourrit également des vulnérabilités mises en exergue par la survenance d'incidents cyber).

Note n°2 : La collecte des « *near miss* » (attaques bloquées par le système de sécurité avant impact sur le SI) présente un intérêt non négligeable. L'analyse de ces incidents permet en effet de repérer les zones d'intérêts des attaquants sur le SI (signaux faibles), ce qui favorise le renforcement préventif des éventuels points faibles de ce dernier.

---

13 « *Security Operations Center* » : système de surveillance centralisé des activités anormales du SI.

14 Par « incident cyber », la mission englobe ici à la fois les incidents « avérés » (ayant eu un impact direct sur le SI de la SGP) et les incidents dits « *near miss* » n'ayant pas eu d'impacts car bloqués par le dispositif de cyber sécurité de la SGP.

Rappel réglementaire :

- La SGP veille à ce que ses dirigeants informent 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. Dans les mêmes conditions, ils informent également l'AMF de tout événement ne permettant plus à la SGP de portefeuille de satisfaire aux conditions de son agrément. Ils fournissent à l'AMF un compte rendu d'incident indiquant la nature de l'incident, les mesures adoptées après sa survenue et les initiatives prises pour éviter que des incidents similaires ne se produisent. La SGP établit une base de données historique, dans laquelle sont enregistrés tous les dysfonctionnements, les pertes et les dommages – articles 321-35 (g) (gestion d'OPCVM) et 318-6 (gestion de FIA) du règlement général de l'AMF.

Bonne pratique :

- Étendre la surveillance automatisée du SI sur la plage horaire la plus large possible (non limitée aux heures ouvrées).

Mauvaise pratique :

- Inclure les incidents cyber dans le processus de gestion des incidents opérationnels, sans clé de classification spécifique (destinée à faciliter l'analyse et le traitement des vulnérabilités sous-jacentes).

4.5- GESTION DES DONNÉES SENSIBLES

Seule la SGP n°3 dispose d'une politique de classification des données selon leur niveau de criticité et d'une cartographie de ses données sensibles. **Les autres SGP n'ont mis en place ni l'une ni l'autre** (les SGP n°2 et 6 bénéficient néanmoins de la politique de classification des données du Groupe).

De ce fait, **l'approche cyber des SGP contrôlées s'appuie davantage sur des modèles** (généralement imposés par le Groupe) **que sur une analyse détaillée, par les SGP, des zones de risques majeures** portées par les données sensibles. Cette approche s'exprime par exemple :

- chez les SGP n°1 et 2 : par une stratégie de continuité d'activité traitant prioritairement les fonctionnalités métier à réactiver post-interruption (par exemple les départements « Front » et « Middle-Office ») et non les données clés à protéger (par exemple l'actif et le passif des fonds) ;
- chez la SGP n°1 : par des approximations dans la cartographie du SI. À titre d'exemple, l'application de suivi des participations est classée en sensibilité 'moyenne' dans la cartographie des systèmes alors qu'elle traite des données confidentielles (par exemple : identité des souscripteurs et notes de gestion sur ces derniers) et devrait de ce fait être classée en sensibilité 'forte'.

L'absence d'un travail d'identification et de classification, *ab initio*, des données sensibles (par exemple : identité des investisseurs, contenu des portefeuilles gérés, stratégies propriétaires d'investissements, données financières des sociétés-cibles[15]), fait courir aux cinq SGP concernées (n°1, 2, 4, 5 et 6) un double-risque. Tout d'abord, celui d'une couverture non-exhaustive de leur SI critique par le dispositif cyber. Ensuite, celui d'un choix erroné des systèmes à protéger prioritairement dans une optique de protection des données et de continuité d'activité.

15 Dans le cas du capital-investissement.

Mauvaise pratique :

↗ Déployer un dispositif de cyber sécurité en l'absence (i) d'identification préalable, (ii) de classification par niveau de criticité (en fonction des critères DICT) et (iii) de revue régulière des données et des systèmes informatiques sensibles.

4.6- GESTION DE LA CONTINUITÉ D'ACTIVITÉ

Comme demandé par la réglementation, **les 6 SGP ont défini un plan de continuité d'activité (PCA[16]).** La mission de contrôle a vérifié que ce dernier **couvre notamment, pour les 6 SGP contrôlées, la perte ou l'indisponibilité du SI** à la suite, notamment, d'une attaque cyber.
Ce PCA est testé annuellement au niveau groupe pour les SGP n°1 et 2. En revanche, le test du PCA s'avère insuffisant pour les 4 autres SGP puisque :

- concernant les SGP n°3 et 4, il se réduit à la vérification des capacités de connexion d'un seul collaborateur sur les installations informatiques de secours, **ce qui ne suffit pas à prouver la capacité de l'ensemble des fonctions clés de la SGP (« *front/middle/back office* », risques et contrôles) à travailler de manière collaborative** en interne et avec l'extérieur, à la suite d'une rupture d'activité causée par une attaque cyber ;
- concernant la SGP n°5, il n'a pas eu lieu depuis plus d'un an ;
- quant à la SGP n°6, les rapports des tests effectués ne font pas apparaître clairement (i) le suivi itératif de la résolution des anomalies constatées et (ii) le mode de sélection du périmètre testé en termes d'applications et d'utilisateurs critiques.

➢ *Installations informatiques de secours*

Des installations informatiques de secours n'ont été identifiées que pour les 4 SGP de l'échantillon appartenant au groupe les plus importants et les plus anciens (SGP n°1, 2, 3 et 6). Ces 4 SGP bénéficient dans ce cadre de sièges dédiés sur le site de secours du groupe lui-même. Pour la SGP n°4, le site de secours est constitué d'un serveur localisé au domicile personnel du président du Groupe, sans garantie solide sur le niveau de sécurité physique des installations. Enfin, la SGP n°5 (qui est indépendante) ne dispose pas de site de secours. Elle a indiqué gérer le risque associé par des sauvegardes régulières de ses données, alors que les supports physiques de ses sauvegardes sont stockées au domicile du président de la SGP, sans garantie suffisante quant à leur niveau de sécurité physique.

La mission de contrôle a noté par ailleurs, dans la stratégie de continuité d'activité de la SGP n°3, la prise en compte pertinente du risque d'attaque(s) cyber directement sur les installations informatiques de secours.

➢ *Test de restauration des données sauvegardées*

Seules les SGP n°1, 4 et 6 réalisent régulièrement un tel test. Pour les SGP n°2 et 3, le groupe réalise lui aussi un test de restauration des données sauvegardées mais à l'échelle de la zone Europe et sur base d'un échantillon aléatoire. Il n'y a donc pas de garantie que les sauvegardes des données des SGP contrôlées soient testées périodiquement par ce biais.

---

[16] Rappel règlementaire : La SGP établit et maintient opérationnels des systèmes et procédures permettant de sauvegarder la sécurité, l'intégrité et la confidentialité des informations de manière appropriée eu égard à la nature des informations concernées. Elle 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 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 - articles 321-24 et 321-25 du règlement général de l'AMF (OPCVM), article 57 2) et 3) du règlement délégué (UE) n°231/2013 (FIA), article 21 2) et 3) du règlement délégué (UE) n° 2017/565 (GSM).

Quant à la SGP n°5, elle ne réalise pas de test de restauration des données sauvegardées. Cette carence est porteuse d'un risque en termes de PCA puique, comme indiqué *supra*, la stratégie de continuité d'activité de la SGP n°5 repose exclusivement sur le processus de sauvegarde régulière de ses données.

Bonne pratique :

↗ Intégrer, dans la stratégie de continuité d'activité de la SGP, la vérification régulière : (i) des capacités de travail collaboratif des équipes clés en situation de crise, (ii) de la capacité à restaurer les données sauvegardées, (iii) du niveau de sécurité physique et informatique des installations de secours.

4.7- DISPOSITIF DE CONTRÔLE DU SI SENSIBLE ET DE LA CYBER SECURITÉ

➢ *Contrôle permanent du SI et du dispositif de cyber sécurité*

Quatre SGP (n°1, 2, 3 et 6) bénéficient d'un contrôle permanent portant sur le dispositif de cyber sécurité. Pour autant, il s'agit de celles qui gèrent les encours les plus importants au sein de l'échantillon. Cette fonction de contrôle est pilotée par le groupe, sauf pour la SGP n°1. Cette dernière a en effet mis en place une ressource dédiée au contrôle permanent cyber **au sein de la direction de la conformité**.

Néanmoins, **le contrôle permanent du dispositif cyber instauré par les quatre SGP citées ci-dessus n'est que partiellement efficace**. En effet :

- concernant la SGP n°1, 30 % des contrôles menés sont systématiquement évalués comme « à surveiller » ou « non satisfaisant » depuis 2016. Ils concernent principalement l'administration et la surveillance du SI (50 %) et la gestion des accès logiques (25 %). Malgré **la récurrence de ces anomalies, aucun plan d'action global n'a été mis en place pour y remédier ;**
- concernant la SGP n°2, le constat est similaire. Les anomalies récurrentes concernent cette fois (i) le défaut de déclaration des licences, (ii) la traçabilité insuffisante des actions de télémaintenance et (iii) l'absence d'une cartographie des données sensibles ;
- **concernant la SGP n°3, aucune information n'est communiquée par le Groupe sur le résultat des contrôles permanents ciblant le SI utilisé par la SGP**. Par ailleurs, les contrôles cyber de premier niveau réalisés localement (ciblant l'accès aux répertoires partagés, les mises à jour des correctifs de sécurité Microsoft, le contrôle des téléchargements et des licences) ne sont pas inclus dans le périmètre du contrôle permanent ;
- **concernant la SGP n°6,** le contrôle permanent du dispositif de cyber sécurité est intégralement réalisé par une équipe Groupe mais sans qu'un suivi formel et consolidé des résultats obtenus ne soit réalisé au niveau de la SGP.

➢ *Contrôle périodique du SI et du dispositif de cyber sécurité*

L'ensemble des SGP contrôlées ont mis en place un contrôle périodique du niveau de cyber sécurité de leur SI (à l'exception de la SGP n°5). Ce contrôle est délégué à un prestataire externe en charge de la réalisation de tests techniques (test d'intrusion, audit de code, audit de configuration). Ce contrôle ne s'avère toutefois que partiellement satisfaisant pour la majorité des 5 SGP concernées (SGP n°3 exclue) puisque :

- **concernant la SGP n°1, le contrôle périodique n'a couvert que 40 % des applications critiques** utilisées par la SGP ;

- **concernant la SGP n°2, 71 % des tests réalisés depuis début 2016 ont été notés « dégradés » ou «insuffisants » de façon récurrente**, sans qu'un projet de remédiation des causes des vulnérabilités identifiées n'ait été mis en place (malgré le niveau de risque important[17] associé à ces vulnérabilités) ;
- **concernant la SGP n°4, le dernier test d'intrusion à avoir été réalisé date de plus de trois ans** (aucun contre-audit n'ayant par ailleurs été réalisé pour vérifier la prise en compte adéquate des mesures de remédiation prises après le test d'intrusion de 2016) ;
- **quant à la SGP n°6**, l'inspection groupe n'a pas réalisé de contrôle périodique de son dispositif de cyber sécurité depuis trois ans.

➢ ***Contrôle des prestataires intervenant sur le SI et le dispositif de cyber sécurité des SGP***

Prestataires internes

Les SGP n°1, 2, 3 et 6 ont bien défini dans une convention de service les prestations attendues de leur groupe d'appartenance en matière de maintenance de leur SI et de cyber sécurité. Ces conventions incluent les indicateurs utilisés par la SGP pour piloter cette prestation ainsi que les moyens de contrôle dont elle dispose.

Toutefois, seule la SGP n°1 s'est dotée de moyens de contrôle efficace des prestations de cyber sécurité rendues par son groupe. Ces moyens prennent la forme d'un contrôleur cyber expert de second niveau rattaché à la directrice de la conformité.

En revanche, les SGP n°2, 3 et 6 ne réalisent pas de contrôle des prestations de cyber sécurité délivrées par leur groupe d'appartenance. À titre d'exemple, elles ne reçoivent pas d'informations quant aux tests techniques menés par le Groupe sur le SI qu'elles utilisent. Elles se trouvent donc dans l'incapacité de juger de l'adéquation du dispositif cyber déployé à leurs activités et risques spécifiques.

La SGP n°4 n'a pas défini de convention de service avec son groupe d'appartenance et ne dispose donc pas de moyens de contrôle sur les services rendus par son groupe en matière de cyber sécurité**.**

Prestataires externes (applications)

L'une des analyses effectuées par la mission de contrôle a porté sur le niveau de risque cyber porté par les systèmes d'information externes traitant les données nécessaires aux fonctions clés de la SGP (passation des ordres, calcul de valorisation, gestion de passif, etc.). Cette analyse a fait apparaître plusieurs tendances :

- **concernant la dépendance au *Cloud***, elle est plus forte, sans surprise, au sein des SGP de petite taille (SGP n°4 et 5). Elle s'avère principalement liée à l'usage des produits de l'éditeur Microsoft ;
- **concernant la dépendance aux éditeurs externes**, elle s'avère notable pour 5 SGP sur 6 (SGP n° 2 à 6). La dépendance à Bloomberg est quant à elle généralisée pour l'ensemble de l'échantillon des SGP contrôlées.

Les applications développées en interne sont minoritaires, sauf pour les deux SGP (n°1 et 2) présentant les encours les plus importants.

Prestataires externes (ressources)

Les SGP n°1, 3, 4, 5 et 6 font appel à des prestataires externes pour intervenir sur leur SI en général et sur leur dispositif de cyber sécurité en particulier[18]. Cette relation est encadrée par un contrat formel pour l'ensemble des prestations concernées. La prestation majoritaire rendue dans ce cadre consiste en la réalisation, par le prestataire externe, d'un test d'intrusion sur le SI de la SGP concernée.

17 Impact potentiel fort, probabilité d'occurrence moyenne à faible.

18 Ce constat s'applique notamment à la SGP n°6 qui compte plus de 50 % d'externes au sein de son département de cyber sécurité.

Dans les faits, **seule la SGP n°3 a mis en place les conditions propices à un contrôle permanent efficace de son principal prestataire externe informatique** (fournisseur de son application de gestion) :

- la mise en place d'un canal d'échange direct entre le prestataire externe et les dirigeants de la SGP ;
- la nomination au niveau groupe d'un chargé de maîtrise d'ouvrage dédié à cette application afin d'appuyer tous travaux d'évolution requis ;
- la réalisation régulière de comités de pilotage de la prestation.

En revanche,

- **les SGP n°1, 4 et 6 n'ont pas intégralement identifié les prestataires informatiques leur délivrant des services essentiels, d'où un contrôle non exhaustif de ces derniers**. À titre d'exemple, la société qui fournit à la SGP n°4 son logiciel de gestion n'était pas identifiée par cette dernière comme un prestataire critique, ce qui a conduit à une absence de contrôle permanent et périodique des services rendus à la SGP ;
- concernant la SGP n°5, la prestation rendue par le prestataire en charge de la maintenance et de la surveillance du SI est contrôlée directement par les dirigeants de la SGP (qui en sont également les donneurs d'ordre) **mais pas par le contrôle permanent de la SGP**.

Par ailleurs, **aucune des quatre SGP citées ci-dessus n'a diligenté d'audit visant la qualité des travaux menés par les prestataires externes intervenant sur son SI ou son dispositif de cyber sécurité**.

Enfin, la SGP n°2 ne fait pas directement appel à des prestataires externes pour intervenir sur son dispositif de cyber sécurité.

➢ ***Assurances contre les risques de cyber sécurité***

Les SGP n°1, 2, 3 et 6 bénéficient d'une assurance spécifique contre les risques cyber, souscrite par leur Groupe d'appartenance. Le plafond des garanties n'est pas proportionnel aux montants des encours gérés puisqu'il varie de 10 M€ (pour la SGP n°1) à 400 M€ (pour la SGP n°3). Les SGP n°4 et 5 n'ont pas souscrit d'assurances spécifiques à ce type de risque.

Rappels réglementaires :

↗ Lorsque la SGP 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. Une tâche ou fonction opérationnelle est considérée comme essentielle ou importante lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement soit à la capacité de la SGP de se conformer en permanence aux conditions et aux obligations de son agrément ou à ses obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier, soit à ses performances financières, soit à la continuité de ses activités. La SGP conserve l'expertise nécessaire pour contrôler effectivement les tâches ou fonctions externalisées, gère les risques découlant de l'externalisation et procède au contrôle de ces tâches et à la gestion de ces risques – articles 321-93 à 321-96 du règlement général de l'AMF (OPCVM), articles 318-58 à 318-61 du règlement général de l'AMF (FIA), article L. 533-10 II 4° du code monétaire et financier et article 30 (1) du règlement délégué (UE) n°2017/565 (GSM).

↗ La SGP établit et maintient opérationnelle une fonction de conformité efficace exercée de manière indépendante. Cette mission consiste notamment à contrôler et, de manière régulière, évaluer l'adéquation et l'efficacité des politiques, procédures et mesures mises en place et des actions entreprises visant à remédier à tout manquement de la SGP et des personnes concernées à leurs obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et

financier. Lorsque cela est approprié et proportionné eu égard à la nature, à l'importance, à la complexité et à la diversité des activités qu'elle exerce, la SGP établit et maintient opérationnelle une fonction de contrôle périodique distincte et indépendante de ses autres fonctions et activités et dont les responsabilités sont les suivantes : 1. établir et maintenir opérationnel un programme de contrôle périodique visant à examiner et à évaluer l'adéquation et l'efficacité des systèmes, mécanismes de contrôle interne et dispositifs de la SGP ; 2. formuler des recommandations fondées sur les résultats des travaux réalisés conformément au 1° ; 3. vérifier le respect de ces recommandations ; 4. fournir des rapports sur les questions de contrôle périodique » – articles 321-31 et 321-83 du règlement général de l'AMF (OPCVM), articles 61(2) et 62 du règlement délégué (UE) n° 231/2013 (FIA), articles 22(2) et 24 du règlement délégué (UE) n°2017/565 (GSM).

Bonne pratique :

- Faire réaliser régulièrement, par un prestataire externe spécialisé, un test d'intrusion sur le SI de la SGP afin de : (i) mesurer la robustesse du dispositif de cyber sécurité en place et (ii) vérifier l'efficacité de prise en compte des vulnérabilités identifiées lors du test antérieur.

Mauvaises pratiques :

- Ne pas définir ni suivre d'indicateurs de pilotage des prestations de maintenance, d'évolution du SI et de gestion de la cyber sécurité au prétexte que celles-ci sont délivrées par le groupe d'appartenance de la SGP.
- Déployer le processus de contrôle permanent/périodique des prestataires informatiques externes sensibles sur la base d'une liste non exhaustive de ces derniers.