DECEMBER 2019

REVIEW OF SPOT INSPECTIONS 2019 CYBERSECURITY SYSTEMS OF ASSET MANAGEMENT COMPANIES

amf-france.org

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

INTRODUCTION

As announced in the AMF's supervision priorities for 2019, the first series of SPOT inspections for 2019 targeting asset management companies ("AMCs") consisted of a review of the cybersecurity systems of five market participants: "*The constant increase in threats has heightened awareness of the implications of cybersecurity for financial market participants. At the end of 2018, the AMF carried out initial survey to review the organisation of the AMCs with regard to IT security […] This initial compilation of information […] will be supplemented in 2019 by SPOT inspections and conventional inspections [targeting the] organisation, procedures and effectiveness of the system deployed to ensure Information Systems governance and security*."

The main purpose of these targeted inspections was to ensure (i) suitable consideration of cyber risks and (ii) the effectiveness of internal controls carried out to address those risks. The choice of this theme was motivated by a combination of numerous risk factors, including the industry's growing dependence on dematerialised facilities and external IT service providers (e.g. Cloud services).

These inspections on the cybersecurity system were carried out simultaneously in five AMCs. The verifications mainly covered the 2016-2018[1] period and examined:

- Organisation of the cybersecurity system for the AMCs inspected (internal/external resources, employee training);
- Governance of this system (Information Systems Security ("ISS") strategy), mapping of IT systems and associated IT risks, procedural corpus, comitology);
- Administration of the Information System ("IS") (workstations, servers, wired network, Wi-Fi, electronic mailing service);
- The IS surveillance system and in particular the IT incident management process (detection, analysis, resolution, *post-mortem* review);
- Management of sensitive data (existence of a policy of data classification by criticality level and a map of these data);
- The business continuity plan (existence of a recovery site, a mirroring system, an IT disaster recovery strategy, review of the regular data backup process, consideration of cyber risks in this strategy);
- Controls in place on the IS (management of data access, changes and IT operation) and the cybersecurity system.

This overview was coordinated with the survey carried out by the AMF Asset Management Department in 2018 on 40 French AMCs. It also used (i) the findings of the conventional inspection carried out in 2019 on the cybersecurity system of an AMC which is a subsidiary of a major French bank, and (ii) information from the survey[2] published by the AFG (French asset management association) in October 2018 on the subject of "*Cybersecurity: what procedures and resources are implemented at AMCs*".

These inspections gave rise to follow-up letters containing requests to remedy the anomalies identified. This overview therefore aims to provide a clarification of the practices of the AMCs under review with regard to the system of cyber control of their sensitive data, their key processes and their Information Systems in general.
This document is neither a position nor a recommendation and may not introduce elements of policy. The practices identified as 'good' or 'bad' are not the expression of an AMF policy. They stress any predominant

1 Several documents provided (in particular security procedures or audit reports) are dated 2019 but cover the Information System as it existed in 2018.

2 Carried out on a sample of 70 AMCs (including 28 subsidiaries of financial groups and 42 entrepreneurial AMCs) having (totally) €4bn in assets under management and employing around 15,000 people.

approaches observed during the inspections, which could facilitate, or complicate[3] the effective and sustainable management of cybersecurity risks and their potential consequences on both the operational and regulatory levels.

CONTENTS

[3] Since a bad practice could be the cause of a failing.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

1- MAIN CONCEPTS AND GLOSSARY

➢ *Definition of cybersecurity risk*

Cybersecurity risk arises from **any potential malicious attack, internal or external, on one of the key features of the Information System of an AMC,** i.e. its availability, its integrity, the confidentiality of the data that it processes, the traceability of users' actions and the non-repudiation of these actions[4]. It is customary to summarise these characteristics by the acronym **AICT (Availability, Integrity, Confidentiality, Traceability)**.
Cybersecurity risk can target collective investments and/or discretionary management portfolios: in that case it is treated as, but is not limited to, an operational risk. Indeed, its materialisation can also result in a regulatory non-compliance[5] of the AMC in areas relating to the existence and maintenance of:

- ☐ the **level of regulatory capital** (since this capital could be adversely affected in the event of a disruption of operations);
- ☐ a **strict policy of retention and maintenance of operational data**, notably with a view to inspections by the AMF (on the transactions performed and anti-money laundering);
- ☐ an appropriate, tested and effective **business continuity plan** (BCP) (since a cyberattack could mean that the AMC's IT infrastructure and/or standby facilities and/or backups are unusable);
- ☐ **appropriate and sufficient (IT) resources**;
- ☐ a **robust system for protection of sensitive data** (relating to investors, funds and mandates).

The analyses of the inspection team on the processes for management of sensitive data did not concern verification of compliance with the GDPR regulation. However, it should be remembered that cybersecurity risk can impact the AMC's compliance with its GDPR obligations when it affects data of a personal nature.

It is also specified that the AMC should be organised so as to inform "*the AMF immediately of any incidents that could lead to a loss or gain for the AMC, a cost linked to its civil or criminal liability, an administrative sanction or reputational damage, resulting from non-compliance with the [general organisation rules] for a gross amount that exceeds 5% of its regulatory capital.*" (Articles 321-35 (UCITS management) and 318-6 (AIF management) of the AMF General Regulation).

➢ *Glossary*

Term	Definition
Active directory	Directory service provided by Microsoft. It is designed to centralise the identification and authentication of a network of Windows workstations and servers, thereby allowing centrally controlled management by administrators of baseware configuration, user rights, and the installation of software and updates.
Strong authentication	Authentication procedure which requires the concatenation of at least two authentication factors, namely what the user knows (e.g. a password) and what he has (e.g. an authentication token).
CERT	Computer Emergency Response Team: centre for alerting and responding to computer attacks[6]
Hacking	Breaching computer defences

[4] Ability of the Information System (IS) to link unambiguously (and without possible dispute) the actions performed in the IS by a user to the IT account of said user. This function is essential to establish with certainty an audit trail of the actions carried out in the IS.
[5] Refer to the box below on the "main legal rules".
[6] The French National Cybersecurity Agency ANSSI specifies the role of these teams on its website: https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/

Term	Definition
Mirroring	Technical device for business continuity allowing real-time replication of the data from one server on another remote server. In the event of a fault on the main server, the Information System can restart rapidly using the mirroring server, with a minimal or even zero risk of loss of data.
Phishing	Technique used by fraudulent operators to obtain personal information with a view to stealing the identity of an individual or an organisation.
Proxy	Computer component acting as an intermediary between the worldwide web and the AMC's Information Systems network in order to facilitate and monitor exchanges.
SOC	Security Operations Centre: centralised system for monitoring abnormal IS activities.
Wi-Fi	Wireless Fidelity: local area network capable of wirelessly connecting several IT devices.

Introductory note:
The good and bad practices identified during inspections (and mentioned below) should be considered in light of the sample of AMCs inspected, namely, for 4 companies out of 6, subsidiaries of large groups having substantial resources.

2- SUMMARY OF THE MAIN FINDINGS OF THE INSPECTION TEAM

The work revealed that all the AMCs inspected have addressed cyber risk by including it in their mapping, by compiling the cybersecurity incidents that they sustain and by calling on specialised service providers to verify the robustness of their IS. These measures ensure a reasonable technical coverage of the main cyber risks, with the exceptions detailed below.

On the other hand, these AMCs do not take into account the potential impacts of the materialisation of cybersecurity risks on their regulatory compliance with regard to (i) the level of own funds, (ii) data retention and (iii) the business continuity plan and resources (IT systems). Most of the AMCs inspected (4/6) limit cyber risk to operational risk only (e.g. the impact on investors).

Moreover, the inspection team observed the frequent lack of exhaustive maps (i) of sensitive data and (ii) of critical systems, and a data classification policy, although these are the essential first bricks of a sustainable cyber policy allowing the appropriate prioritisation of security measures.

Moreover, the formal identification of cyber incidents, for continuous assessment of the associated risk level, proves problematic. For example, proven cybersecurity incidents (e.g. having impacted the IS) are frequently confused, in the compilation databases, with external attacks that were blocked successfully by the supervision system and/or with basic and unintentional internal computer incidents (e.g. server crash).

Also, for AMCs belonging to a Group (5/6, including 4 belonging to large groups), inadequate supervision of the services (relating to IT, cybersecurity and business continuity) rendered by the parent company was identified. On the one hand, these general services enable the subsidiary AMCs to benefit from the group's expertise and resources. However, they are based on the generic model of the parent company, without making sufficient consideration of the specific business and regulatory features of the AMC subsidiary.

This AMC/Group porosity generates high-risk situations from a technical viewpoint (for example, the interlinking of the AMC's computer network with that of the Group, exposing the former directly in the event of an attack on the latter) and from an organisational viewpoint (e.g. the AMC's lack of visibility regarding the exhaustiveness and effectiveness of the services rendered by the Group such as data backup and intrusion tests). It also leads the AMCs in question to skimp on the direct supervision of their cyber risks, pretexting their lack of in-house expertise compared with the Group's resources. And yet, the main work of highest priority for protection from cyber risks is the responsibility of the AMC. Moreover, since this work is, in practice, of an organisational and procedural nature, it can be undertaken by small-sized companies. The technical work, although it is real, comes only in second place and, once the previous work has been performed, it can indeed be delegated to specialised third parties.

3- CONTEXT AND SCOPE

3.1- INTRODUCTION

In France, the concept of cybercrime was initially defined in the French Data Protection Act of 1978. This concept was subsequently refined in several successive laws between 1988 (Godfrain Act on computer fraud) and 2006 (Anti-Terrorism Act). Within this framework, in 2009 France set up the French National Cybersecurity Agency ANSSI in the Secretariat General for National Defence and Security.

The AMF takes part in workshops on cybersecurity risks via several international working groups (in conjunction with Banque de France and the Treasury Department) such as the G7's Cyber Expert Group (CEG), the Financial Stability Board (FSB) and the European Systemic Cyber Group (ESCG) of the ESRB (European Systemic Risk Board).

At the European level, **the European Supervisory Authorities** (ESAs)[7] **issued joint advice in February 2019 concerning cybersecurity (equivalent to a legislative motion).**[8] This advice mentions the need for **greater harmonisation** of the rules (i) for local governance of cybersecurity and (ii) **for identification, compilation and reporting of cyber incidents to the regulators**. It also refers to the need for a common control grid for the members concerning **supervision of the providers of critical IT services, notably those providing cloud computing services**. Lastly, it suggests the gradual establishment of a coherent and proportionate framework for **technical testing of the cyber resilience of regulated institutions**, by performing intrusion tests.

3.2- PRESENTATION OF THE SAMPLE OF AMCS INSPECTED

The AMCs selected for these thematic inspections were picked in order to establish a sample group of marketplace practices concerning cybersecurity systems in asset management:

- AMC 1 is the subsidiary of a French banking group. It is specialised in private equity investment and manages FPCI and FPS funds;
- AMC 2 is the subsidiary of a French AMC. It is specialised in money market fund management;
- AMC 3 is the subsidiary of a US bank. It is specialised in passive management;
- AMC 4 is the subsidiary of a French finance group. Unlike the three AMCs above, it focuses mainly on retail clients;
- AMC 5 is an entrepreneurial company.

In parallel to the SPOT assignments, in 2019 the AMF also inspected another AMC, which is a subsidiary of a French bank, on the subject of cybersecurity. The results of this 'conventional' inspection have been included in the following sections for the purpose of comparison with the sample of AMCs inspected within the framework of the SPOT assignment. The AMC in question is No. 6.

The investigations covered the period from 1 January 2016 to 31 December 2018.

3.3- APPLICABLE REGULATIONS

The work of the inspection team was based on:

- the AMF General Regulation;

---

7 The ESAs (European Supervisory Authorities) consist of ESMA (European Securities and Markets Authority), the EBA (European Banking Authority) and EIOPA (European Insurance and Occupational Pensions Authority)

8 This advice can be accessed via: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

- ☐ the Monetary and Financial Code;
- ☐ Delegated Regulation (EU) No. 231/2013 of the AIFM Directive;
- ☐ Delegated Regulation (EU) No. 2017/565 of the MiFID II Directive.

Main legal sources

Organisation rules

a) Article 321-23 (I)(II)(IV)(VI) of the AMF General Regulation (UCITS), Article 318-1 of the AMF General Regulation, Article 57 (1) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 21 (1) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the appropriate and sufficient material, financial and human resources which the AMC must have;**

b) Article 321-23 (III)(V) of the AMF General Regulation (UCITS), Articles 22 and 57 (1 b) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 21 (1)(b)(d) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **AMCs' employment of personnel having the required skills, knowledge and expertise;**

c) Articles 321-83 of the AMF General Regulation (UCITS), Article 62 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 24 of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the establishment and maintenance of a periodic control function operating independently;**

d) Article 321-25 of the AMF General Regulation (UCITS), Article 57 (3) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 21 (3) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the establishment and maintenance of a business continuity plan aimed at ensuring, in the event of a disruption of their systems and procedures, the preservation of essential data and the maintenance of investment services and activities.**

Compliance system

e) Article 321-30 of the AMF General Regulation (UCITS), Articles 318-4 of the AMF General Regulation and 61 (1) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Articles 312-1 of the AMF General Regulation and 22 (1) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the establishment and operational maintenance of adequate policies, procedures and measures designed to detect any non-compliance risk;**

f) Article 321-31 of the AMF General Regulation (UCITS), Article 61 (2) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 22 (2) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the establishment of an effective compliance function operating independently.**

Responsibility of senior management

g) Article 321-35 (g) of the AMF General Regulation (UCITS management) and Articles 318-6 of the AMF General Regulation and 13 (2) of Delegated Regulation (EU) No. 231/2013 (AIF management) concerning **incident compilation and associated notification of managers and the AMF**;

h) Article 321-36 of the AMF General Regulation (UCITS), Article 60 (4) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 25 (2) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **regular notification of management regarding the results of permanent and periodic controls.**

Risk management

j) Article 321-77 of the AMF General Regulation (UCITS), Articles 38 and 39 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 23 of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the establishment of a risk management function operating independently;**

i) Articles 321-78 et 321-79 of the AMF General Regulation (UCITS), Article 40 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Articles 312-46 of the AMF General Regulation and 23 of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning the **establishment and operational maintenance of an appropriate and documented risk management policy designed to determine the risks to which collective investment products and individual portfolios are or could be exposed;**

k) Articles 321-35 and 321-80 of the AMF General Regulation (UCITS), Articles 41 and 60 (2) of Delegated Regulation (EU) No. 231/2013 (AIFs), Article 312-47 of the AMF General Regulation and Article 25.1 of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the regular audit of risk management policies and procedures;**

l) Article 321-81 of the AMF General Regulation (UCITS), Article 39 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 312-48 of the AMFGR (investment firms) concerning **constant measuring and management of the risks to which collective investment products and individual portfolios are or could be exposed;**

m.1) Article 321-76 of the AMF General Regulation (UCITS), Article 13 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 312-44 of the AMF General Regulation (investment firms) concerning the **definition of the operational risk of loss for collective investment products or individual portfolios;**

m.2) Article 13 of Delegated Regulation (EU) No. 231/2013 (AIFs) concerning the **definition of operational risk for the AIFM AMC.**

Outsourcing

n) Articles 321-93 to 321-96 of the AMF General Regulation (UCITS), Articles 318-58 to 318-61 of the AMF General Regulation (AIFs), Article L.533-10 II 4°of the Monetary and Financial Code and Article 30 (1) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **outsourcing of essential services.**

Data recording and retention

o) Article 321-24 of the AMF General Regulation (UCITS), Article 57 (2) of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 21 (2) of Delegated Regulation (EU) No. 2017/565 (investment firms) concerning **the obligation to safeguard the security, integrity and confidentiality of the information processed by the AMC;**

p) Articles L. 533-8 and L. 533-10 II 6° of the Monetary and Financial Code relating to the **obligation of retention of relevant information associated with the transactions performed;**

q) Articles 321-69 to 321-74 of the AMF General Regulation (UCITS), Articles 57 (1), 58 and 64 to 66 of Delegated Regulation (EU) No. 231/2013 (AIFs) and Article 312-41 of the AMF General Regulation and Article 75 of Delegated Regulation (EU) No. 2017/565 (investment firms) relating to **recording and retention of the data needed for auditing the operations performed by the AMC.**

4- OBSERVATIONS AND ANALYSES

In the SPOT inspection approach, three types of observations can be expressed: breaches (like for 'conventional' inspections) and good or bad practices.

A **breach of the regulations** reflects an identified failure to comply with a specific text of the regulations (which will be referred to in the overview).

Good and bad practices were defined in the introduction to this document.

4.1- CYBERSECURITY SYSTEM ORGANISATION AND MEANS EMPLOYED

➢ *Independence of the cybersecurity function*

The Information System ("IS") of the five AMCs in the inspected sample belonging to a Group (Nos. 1, 2, 3, 4 and 6) is included in the Group's IS. Accordingly, it is the Group that is in charge of maintenance, upgrading and supervision of the AMC's IS. AMC 3 is the only one of the five to follow a different approach as it uses an external management application (supplied by a French software publisher) which is not a Group standard.

Within this framework, **the IS of four of these five AMCs is managed by the Group CIO and controlled by the Group's Chief Information Security Officer ("CISO")** (the recruitment of an in-house CISO is in progress at AMC 4). This reliance on the Group goes hand-in-hand with considerable dependence on outside service providers for AMCs 1, 3 and 4, mainly due to the business applications used by these AMCs. In contrast, AMC 6 has its own CIO and CISO.

For AMCs 1, 2, 3 and 6, **the independence of the CISO function relative to the CIO** is ensured by:

- Administrative or functional reporting by the Group CISO to the Executive Committee (for AMCs 2, 3 and 6);
- The existence of an independent control function (reporting to Compliance) of the CISO (for AMC 1).

AMC 5, the only independent AMC, has neither an IS Department nor a CISO. It is completely dependent on a single outside IT service provider (present since the founding of the AMC) for maintenance, upgrading and cyber surveillance of its IS. This service provider performs this work under the supervision of the AMC's CEO.

➢ *Budget of the cybersecurity system relative to the IS Department*

Monitoring of the "budget allocated to cybersecurity/budget of the IT function" ratio is a cybersecurity system management indicator useful to the AMC's management. It makes it possible to measure changes in the consideration of cyber risk (by performing outsourced intrusion tests, for example) in overall IT spending (which covers, for example, the replacement of servers).

The inspection team notes, in this context, that IT spending is correctly identified for all the AMCs inspected. AMCs 1, 2 and 4 were also able to provide the "cyber budget/IS Department budget" ratio calculated at the level of their parent Group (it ranges between 1% and 3 %). AMC 6, for its part, was able to provide this ratio (calculated on its own level): the cyber budget of this AMC represented 6% of its IS Department's budget in 2018.

➢ *Raising personnel's awareness of cybersecurity risks*

Employee awareness raising programmes have been organised only in the four AMCs of the sample having the largest assets under management (i.e. AMCs 1, 2, 3 and 6).

However, for AMCs 1 and 2, these programmes do not include phishing tests. AMCs 3 and 6, which have established this type of test, have an effective tool for supervision of changes in the level of employees' vigilance (which enables them notably to step up training for the populations whose results in the tests show that they need it).

In AMC 6, there is no consolidated overall monitoring making it possible to measure changes in the level of cybersecurity risk awareness among users of the IS.

Regulatory reminder:

- The AMC shall ensure that their relevant persons are aware of the procedures which must be followed for the proper discharge of their responsibilities. It shall employ personnel with the required skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them", Article 321-23 III and V of the AMF GR (UCITS), Articles 22 and 57(1b) of Delegated Regulation (EU) No. 231/2013 (AIFs), and Article 21 1) b) and d) of Delegated Regulation No. 2017/565 (investment firms).

Good practices:

- Ensuring the independence of the CISO function relative to the IS Department either by (administrative or functional) reporting by the CISO to the Executive Committee, or by establishing a control function independent of the CISO's activities.
- Raising the AMC's employees' awareness of cybersecurity risks by including them in the annual training plan and, at least once a year, performing a phishing test (structured differently from one year to the next) on all the AMC's employees to verify changes in their level of sensitivity to cyber risks.
- In the AMC's annual IT spending, distinguishing spending related to cybersecurity.

4.2- CYBERSECURITY SYSTEM GOVERNANCE

➢ ***Cybersecurity strategy***

AMCs 2, 3, 5 and 6 organise their cybersecurity system around a clear, formalised strategy, validated by the Executive Committee of the Group (for AMCs 2, 3 and 6) or of AMC 5. This approach has the advantage of providing a permanent formal framework for cybersecurity work, prioritising the work according to risks defined beforehand as of highest priority and making them accessible to non-specialists (internal and external).
AMCs 2, 3 and 6 apply the strategy of their parent Group. AMC 5 (which is independent) has defined its own strategy, in line with its limited resources and its main risks. This is based on:

- maintenance of an installed base of hardware and software that is up-to-date and homogeneous;
- segregation of data access and sensitive transactions;
- pre-emptive analysis of the risk of a disruption of operations.

Conversely, **AMCs 1 and 4 have not defined a cybersecurity strategy.**

The cybersecurity strategies of the AMCs inspected are based on the marketplace reference documents presented below. The inspection team noted that the reference documents most commonly used were the hygiene guide of the ANSSI and the NIST reference document[9] (in particular by AMC 6).

[9] *National Institute of Standards and Technology*: a body of the *US Department of Commerce* which has developed an international cybersecurity reference document.

Name	Issuer	Link
« Le guide d'hygiène » (hygiene guide)	ANSSI	https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
« Guide de la sécurité des données personnelles » (Guide to personal data security)	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
Standards 27001 and 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 (list of 20 cybersecurity controls breaking down into 6 'basic', 10 'foundational' and 4 'organisational' controls)	CIS *Center for Internet Security*	https://www.cisecurity.org/controls/cis-controls-list/

However, the inspection team observes that the Group's cyber strategy is applied directly by AMCs 2, 3 and 6 **without a clear margin for adaptation regarding consideration of their specific regulatory and operational features**. For instance, the inspection team did not identify in the documents provided (committee materials or risk analysis sheets) any evidence of the existence of such adaptations. But, since the parent company of each of these AMCs respectively is a bank, there is here a risk of inadequacy of the security measures taken with regard to the real issues facing the three companies in question. This is especially notable, moreover, in that the cybersecurity services rendered by the Group are not sufficiently controlled by these AMCs (refer to Section 4.7 of this overview).

- ***Cyber risk management by the AMCs' management bodies***

In all the AMCs inspected, cybersecurity risks are adequately managed by the management bodies. The six AMCs inspected have appointed in their respective Executive Committees a representative in charge of these risks. This means:

- the chairman of the AMC for AMCs 3 and 5;
- the company secretary for AMCs 2 and 4;
- the Deputy Managing Director in charge of finance for AMC 1;
- a Deputy CEO for AMC 6.

Moreover, AMCs 1, 2 and 6 have strengthened their management of these risks by including them in dedicated committees.

- ***Cybersecurity risk management tools***

These tools are incomplete for all of the inspected sample (except for AMC 6 which applies the procedures of its parent Group), whether for risk mapping or the procedural corpus.

Regarding mapping, only AMCs 1 and 6 have carried out an exhaustive operation:

- Taking account, in their analysis, of the potential impacts of cyber risks in terms of non-compliance of the AMC (i) with the declaration of means of the programme of activity, (ii) with the required level of regulatory capital, (iii) with the retention, integrity and confidentiality of sensitive data (relating to investors, instruments and transactions in particular) and (iv) with the operational maintenance of a robust BCP;
- By also analysing these impacts in terms of financial losses and reputational damage (the latter analysis proving extremely thorough for AMC 6).

The five other AMCs have in their respective mapping operations a simplistic approach to cyber risk by confining it to operational risk only, unrelated to the numerous regulatory breaches that the materialisation of such a risk may entail.

Regarding the procedural corpus on cybersecurity, it proves to be complete only for AMCs 2 and 3 (at the Group level). In particular:

- AMC 1 has no up-to-date procedures relating to the administration of its fixed/mobile IT hardware and its Wi-Fi network;
- AMC 4 has not established a procedure for management of cyber incidents;
- AMC 5 deals with cyber risk in its corpus only from the (simplistic) viewpoint of a disruption of operations.

These shortcomings suggest a risk of insufficient coverage of the cybersecurity risks which could impact the AMCs inspected.

Regulatory reminder:

- AMCs shall establish, implement and maintain policies and procedures designed to detect any risk of failure to comply with their professional obligations and shall put in place measures or procedures to attenuate those risks - Article 321-30 of the AMF General Regulation (UCITS), Articles 318-4 of the AMF General Regulation and 61 (1) of Delegated Regulation (EU) No. 231/2013 (AIFs), and Articles 312-1 of the AMF General Regulation and 22 (1) of Delegated Regulation (EU) No. 2017/565 (investment firms).

Bad practices:

- For AMCs that are Group subsidiaries, basing the cybersecurity system on a Group strategy applied in a top-down manner without sufficient consideration of the specific business and regulatory features of asset management operations in France.
- In AMC risk mapping, confining the analysis of cybersecurity risks solely to the impacts of operational risk on the funds and/or portfolios managed.

4.3- INFORMATION SYSTEM ADMINISTRATION

➢ ***Network compartmentalisation***

The inspection team notes that the five AMCs belonging to a Group (AMCs 1, 2, 3, 4 and 6) are integrated into the Group's computer network. This configuration extends as far as the full integration of their Active Directory (AD)

into that of the Group, which – for equivalent means of protection - could increase the exposure of the AMCs in question to cyber risk in the event of insufficient AD security management by the Group.[10]

The inspection team also identified (notably for AMC 4) an area of potential risk in the integration, on the same IT infrastructure, of several companies of a given group performing different businesses (for example: AMC – business 1 – and corporate banking – business 2). Now, **in the event of ineffective management – at the Group level – of data access rights to the common IS**, such an integration could facilitate unauthorised access by the users of business 1 to the sensitive data of business 2, violating the "Chinese wall" supposed to keep these two businesses separate.

- ***IS administration process***

AMCs 1, 2, 4 and 5 have several shared major vulnerabilities concerning both fixed and nomad workstations and the network. These vulnerabilities (which have been identified by the AMCs themselves) are summarised below.

Identified vulnerabilities	Risks entailed	AMC 1	AMC 2	AMC 4	AMC 5
Missing or incomplete **IS administration** procedures	If not homogeneous (from the viewpoint of application or antivirus software versions, for example), this could facilitate the creation of entry points for an external attacker	X			
Inventories of missing or incomplete fixed or nomad **equipment**			X		
USB ports not blocked on fixed workstations	Data theft and/or injection into the IS of a virus contained in a USB key	X		X	X
No proxy within the framework of internet connections by the AMC's employee	Downloading (non-detectable) by employees of infected files from potentially harmful websites			X	X
Process of **remote network connection** to the IS insufficiently secure and controlled (lack of strong authentication, weak protocols)	Access to the AMC's IS by an external attacker masquerading as an internal user	X		X	

The information collected from AMCs 3 and 6 provided the inspection team with a reasonable assurance that the vulnerabilities identified above do not impact their respective Information System.

Good practice:

- Establishing IS administration procedures for all the equipment used (hardware and network).
- Setting out formally and updating regularly an inventory of the IT equipment used.
- Establishing control of internet logins by in-house employees (including navigation traceability) and control of remote network connection to the IS.

Bad practice:

- Not blocking the USB ports of user workstations.

[10] The active directory (AD) is defined in the glossary at the start of this overview.

4.4- INFORMATION SYSTEM SURVEILLANCE

The six AMCs inspected have defined and established a process for supervision of their Information System. For example, AMCs 2, 3, 5 and 6 enjoy a broad period of supervision (24/24 7/7) of their IS (through the Group "SOC"[11] for AMCs 2, 3 and 6, and via the external IT service provider for AMC 5). However, this process proves satisfactory for only three of the six AMCs inspected (AMCs 2, 5 and 6). In particular:

- **In the case of AMCs 1 and 4, supervision of the IS active only on working days, during the period 7.00 am – 7.00 pm** (except, for AMC 1, on the equipment used by the AMC's managers). This results in a risk of belated reaction in the event of a cyberattack occurring outside of working hours, with a risk of irremediable damage to the targeted IS;
- **In the case of AMC 3, it receives no information concerning the results of the supervision operations carried out on its IS by the Group** (threats detected, attacks countered, etc.).

➢ *Cyber incident management processes*

The six AMCs inspected have defined and established a process for management of cybersecurity incidents.[12] This process proves robust for AMCs 2, 5 and 6. For the other three AMCs inspected:

- **In the case of AMC 1, cyber incidents are not easily identifiable in the database for compilation of all incidents given the lack of a unique identification key**;
- **In the case of AMC 3, it receives no information concerning the handling of cyber incidents which targeted the Group's IS.** This hampers the AMC in its potential understanding of the cyber threats weighing on its operations and therefore interferes with its ability to protect itself from such threats;
- **In the case of SGP 4, it has not established a database classifying the cyber incidents** that it has sustained and dealt with.

An analysis of the volume of cyber incidents reported by each of the AMCs inspected shows that control of the process of compilation of cyber incidents is still imperfect. In particular:

- **AMCs 1 and 2, although they have similar volumes of assets under management** (€27.2bn and €25.2bn) and both belong to a Group, **report 502 and 4 incidents respectively** over the period covered by the inspection. This difference can be explained by the compilation for AMC 1 of proven cyber incidents and attacks that were blocked by the cybersecurity system, whereas AMC 2 only compiles proven incidents;
- **AMC 3, over the same period, states that it experienced no cyber incident**, explaining this by indicating that it has no website and no direct contact with clients;
- AMC 5 mentions 89 cyber incidents occurring on its IS in 2018, but an analysis of these incidents **shows that these are generally conventional IS maintenance operations** (e.g. a change of server or updating of antivirus software);
- As for AMC 6, it **has up to three different reporting databases** in which cybersecurity incidents can be entered. These three databases cover (i) suspected data leaks, (ii) cyber incidents affecting the AMC and (iii) those affecting the Group, respectively. However, there is no single analysis key capable of simply consolidating the data in these databases, and this adversely affects visibility regarding changes in the cyber risk level.

Note 1:
The shortcomings identified above in the compilation of cyber incidents could detract from the exhaustiveness of the cyber risk mapping (to the extent that the latter is also nurtured by the vulnerabilities highlighted by the occurrence of cyber incidents).

---

11 *Security Operations Center*: centralised system for monitoring abnormal IS activities.

12 The inspection team includes in "cyber incidents" both "proven" incidents (having had a direct impact on the AMC's IS) and so-called *near miss* incidents which had no impact because they were blocked by the AMC's cybersecurity system.

Note 2:
The compilation of "near misses" (attacks blocked by the security system before impacting the IS) is of significant interest. An analysis of these incidents makes it possible to identify attackers' areas of interest on the IS (weak signals), which encourages the preventive strengthening of any weak points in the IS.

Regulatory reminder:

- The AMC shall ensure that its managers immediately inform the AMF of any incidents that could lead to a loss or gain for the AMC, a cost linked to its civil or criminal liability, or an administrative sanction or reputational damage, resulting from non-compliance with the [general organisation rules] for a gross amount that exceeds 5% of its regulatory capital. Under the same conditions, they shall also inform the AMF of any event preventing the AMC from meeting the requirements of its authorisation. They shall provide the AMF with an incident report indicating the nature of the incident, the measures implemented after it happened and the initiatives taken to prevent similar incidents from taking place in the future. The AMC establishes an historical database in which are recorded all malfunctions, losses and damage. – Articles 321-35 (g) (UCITS management) and 318-6 (AIF management) of the AMF General Regulation.

Good practice:

- Extending automated supervision of the IS to the broadest possible time range (not limited to business hours).

Bad practice:

- Including cyber incidents in the operating incident management process, without a specific classification key (designed to facilitate the analysis and handling of the underlying vulnerabilities).

4.5- MANAGEMENT OF SENSITIVE DATA

Only AMC 3 has a policy of data classification according to their level of criticality and mapping of its sensitive data. **The other AMCs have established neither one nor the other** (although AMCs 2 and 6 benefit from the data classification policy of their Group).

As a result, **the cyber approach of the AMCs inspected is based more on models** (generally imposed by the Group) **than on a detailed analysis by the AMCs of the major risk areas** resulting from sensitive data. This approach is expressed, for example:

- in AMCs 1 and 2: by a business continuity strategy dealing chiefly with the business functionalities to be reactivated post-interruption (e.g. the front- and middle-office departments) and not the key data to be protected (for example, the funds' assets and liabilities);
- in AMC 1: by approximations in IS mapping. For example, the equity investment monitoring application is classified as of 'average' sensitivity in the systems map, although it handles confidential data (for example, identity of the investors and management notes on the latter) and should therefore be classified as of 'high' sensitivity.

The absence of work on the identification and classification of sensitive data from the outset (e.g. identity of investors, content of the portfolios managed, proprietary investment strategies, financial data of the target companies)[13] means that the five AMCs in question (1, 2, 4, 5 and 6) run a twofold risk. First, the risk of non-

[13] In the case of private equity

exhaustive coverage of their critical IS by the cyber system. Next, the risk of an incorrect choice of systems to be protected in priority from a data protection and business continuity perspective.

> **Bad practice:**
>
> ↗ Deploying a cybersecurity system in the absence of (i) prior identification, (ii) classification by criticality level (on the basis of the AICT criteria) and (iii) regular review of sensitive data and Information Systems.

4.6- BUSINESS CONTINUITY MANAGEMENT

As required by the regulations, **the six AMCs have defined a business continuity plan (BCP).**[14] The inspection team checked that the latter **covers in particular, for the six AMCs inspected, the loss or unavailability of the IS**, notably following a cyberattack.
This BCP is tested once a year at the Group level for AMCs 1 and 2. However, the BCP test proves insufficient for the other four AMCs because:

- In the case of AMCs 3 and 4, it consists merely of a verification of the capability for connection of a single employee to the backup IT systems, **which is not sufficient to prove the capability of all the key functions of the AMC, (front/middle/back office, risks and controls) for working collaboratively** internally and with the outside world, following a disruption of operations caused by a cyberattack;
- In the case of AMC 5, this test has not taken place for more than a year;
- As regards AMC 6, the reports on the tests performed do not show clearly (i) the iterative follow-up of resolution of the detected problems and (ii) the method of selection of the tested area in terms of critical applications and key users.

➢ ***Backup IT systems***

Backup IT systems were only identified for the four AMCs of the sample belonging to the biggest and oldest Groups (AMCs 1, 2, 3 and 6). In this context, these four AMCs have dedicated seats on the recovery site of the Group itself. For AMC 4, the recovery site consists of a server located in the personal home of the Group's chairman, with no solid guarantee regarding the system's level of physical security. Lastly, AMC 5 (which is independent) has no recovery site. It stated that it managed the risk involved by making regular backups of its data, although the physical media for its backups are stored at the home of the AMC's chairman, with no adequate guarantee regarding their level of physical security.

The inspection team also noted, in the business continuity strategy of AMC 3, appropriate consideration of the risk of cyberattack(s) directly on the backup IT systems.

➢ ***Backup data restoration test***

Only AMCs 1, 4 and 6 perform such a test regularly. For AMCs 2 and 3, the Group also performs a backup data restoration test, but on the Europe regional scale and on the basis of a random sample addressing all European

[14] Regulatory reminder: The AMC shall establish and maintain effective systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question. It shall establish and maintain effective business continuity plans aimed to ensure, in the case of an interruption to their systems and procedures, the preservation of essential data and functions, and the maintenance of their UCITS management activity, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their activities - Articles 321-24 and 321-25 of the AMF General Regulation (UCITS), Article 57 2) and 3) of Delegated Regulation (EU) No. 231/2013 (AIFs), and Article 21 2) and 3) of Delegated Regulation (EU) No. 2017/565 (investment firms).

subsidiaries. There is therefore no guarantee that the data backups of the AMCs inspected are tested regularly in this way.
As regards AMC 5, it performs no backup data restoration test. This shortcoming entails a BCP risk because, as indicated above, the business continuity strategy of AMC 5 is based exclusively on the process of regular backups of its data.

Good practice:

↗ Including, in the AMC's business continuity strategy, the regular verification of: (i) the collaborative working capacity of key personnel in a crisis situation, (ii) the ability to restore backup data, and (iii) the level of physical and IT security of the backup systems.

4.7- CONTROL SYSTEM FOR SENSITIVE IS AND CYBERSECURITY

➢ *Permanent control of the IS and cybersecurity system*

Four AMCs (1, 2, 3 and 6) have a permanent control of the cybersecurity system. However, these are the AMCs in the sample having the largest assets under management. This control function is managed by the Group, except for AMC 1. The latter has established a resource dedicated to permanent cyber control **in the Compliance Department**.

However, **the permanent control of the cyber system established by the four AMCs mentioned above is only partially effective**. In particular:

- In the case of AMC 1, 30% of the controls conducted have been systematically assessed as "to be monitored" or "not satisfactory" since 2016. They mainly concern the administration and management of the IS (50%) and data access management (25%). Despite **the recurrence of these problems, no overall action plan has been established to correct them;**
- In the case of AMC 2, the situation is similar. This time the recurring problems concern (i) failure to declare licences, (ii) insufficient traceability of remote maintenance activities, and (iii) the lack of a sensitive data map;
- **In the case of AMC 3, no information is disclosed by the Group regarding the result of the permanent controls targeting the IS used by the AMC**. Moreover, the first-level cyber controls performed locally (targeting access to shared directories, updating of Microsoft security patches, and control of downloading and licences) are not included in the permanent control scope;
- **In the case of AMC 6,** permanent control of the cybersecurity system is carried out entirely by a Group team, but without any formal, consolidated follow-up of the results obtained being performed at the AMC level.

➢ *Periodic control of the IS and cybersecurity system*

All the AMCs in the inspected sample have established a periodic control of the cybersecurity level of their IS (except for AMC 5). This control is delegated to an outside service provider in charge of performing technical tests (intrusion test, code audit, configuration audit). However, this control proves only partially satisfactory for most of the five AMCs in question (AMC 3 excluded) because:

- **In the case of AMC 1, the periodic control covered only 40% of the critical applications** used by the AMC;

- **In the case of AMC 2, 71% of the tests carried out since the start of 2016 were recurrently scored as "degraded" or "insufficient"**, without a plan having been put in place to remediate the causes of the identified vulnerabilities (despite the significant level of risk[15] entailed by these vulnerabilities);
- **In the case of AMC 4, the last intrusion test to have been performed was more than three years ago** (and moreover, no counter-audit was performed to check that the remediation measures taken after the 2016 intrusion test were suitably allowed for);
- **As regards AMC 6**, Group Inspection has performed no periodic control of its cybersecurity system for the past three years.

➢ ***Control of service providers performing work on the AMC's IS and cybersecurity system***

Internal service providers

AMCs 1, 2, 3 and 6 have clearly defined in a service level agreement the services expected of their parent Group with regard to maintenance of their IS and cybersecurity. These agreements include the indicators used by the AMC to manage this service and the means of control at its disposal.

However, only AMC 1 has acquired effective means of control of the cybersecurity services rendered by its Group. These means take the form of a level-two expert cyber controller reporting to the Compliance Director.

On the other hand, AMCs 2, 3 and 6 perform no control over the cybersecurity services provided by their parent Group. For example, they receive no information concerning the technical tests conducted by the Group on the IS that they use. They are therefore unable to assess the suitability of the cyber system deployed for their specific operations and risks.

AMC 4 has not defined a service agreement with its parent Group and therefore has no means of control over the services rendered by its Group on matters of cybersecurity.

Outside service providers (applications)

One of the analyses performed by the inspection team concerned the level of cyber risk generated by external Information Systems processing the data necessary for the AMC's key functions (placing orders, calculation of valuations, liability management, etc.). This analysis showed several trends:

- **Regarding dependence on the Cloud**, not surprisingly it is stronger in the small AMCs (AMCs 4 and 5). It proves to be mainly related to the use of products from the software publisher Microsoft;
- **Regarding dependence on outside software publishers**, it proves significant for five out of six AMCs (AMCs 2 to 6). Dependence on Bloomberg, for its part, is widespread for the whole sample of AMCs inspected.

Applications developed internally are in the minority, except for the two AMCs (1 and 2) having the largest assets under management.

Outside service providers (resources)

AMCs 1, 3, 4, 5 and 6 call on outside service providers to perform operations on their IS in general and on their cybersecurity system in particular.[16] This relationship is governed by a formal contract for all the services in question. The majority of services rendered in this framework consists of the performance, by the outside service provider, of an intrusion test on the IS of the AMC in question.

In practice, **only AMC 3 has established propitious conditions for effective permanent control of its main outside IT service provider** (supplier of its management application):

15 Major potential impact, medium to low probability of occurrence.

16 This observation applies notably to AMC 6 which has more than 50% of outside contractors in its cybersecurity department.

- Establishment of a channel for direct exchange between the outside service provider and the managers of the AMC;
- Appointment, at the Group level, of an overall manager dedicated to this application in order to support all required upgrading work;
- Regular setting up of service steering committees.

On the other hand,

- **AMCs 1, 4 and 6 have not fully identified the IT service providers which provide them with essential services, resulting in non-exhaustive control of the latter**. For example, the company which provides AMC 4 with its management software was not identified by the latter as a critical service provider, which resulted in an absence of permanent and periodic controls of the services rendered to the AMC;
- In the case of AMC 5, the service rendered by the service provider in charge of IS maintenance and supervision is controlled directly by the managers of the AMC (who are also the orderers), **but not by the AMC's permanent control**.

Moreover, **none of the four AMCs mentioned above has conducted an audit concerning the quality of the work carried out by the outside service providers performing work on its IS or its cybersecurity system**.

Finally, AMC 2 does not call directly on outside service providers to work on its cybersecurity system.

➢ ***Insurance against cybersecurity risks***

AMCs 1, 2, 3 and 6 have a specific insurance against cyber risks, taken out by their parent Group. The guarantee cap is not proportional to the amount of assets under management, because it ranges from €10m (for AMC 1) to €400m (for AMC 3). AMCs 4 and 5 have not taken out specific insurance for this type of risk.

Regulatory reminders:

↗ If AMCs outsource the execution of critical operational tasks and functions that are important for the provision of a service or the conduct of business, they shall take reasonable measures to prevent an undue exacerbation of operating risk. An operational task or function shall be regarded as critical or important if a defect or failure in its performance would materially impair the AMC's capacity for continuing compliance with the conditions and obligations of its authorisation or its professional obligations referred to in II of Article L. 621-15 of the Monetary and Financial Code, or its financial performance, or the continuity of its business. AMCs must retain the necessary expertise to supervise the outsourced tasks or functions effectively and manage the risks stemming from outsourcing and must supervise those tasks and manage those risks – Articles 321-93 to 321-96 of the AMF General Regulation (UCITS), Articles 318-58 to 318-61 of the AMF General Regulation (AIFs), Article L. 533-10 II 4° of the Monetary and Financial Code and Article 30 (1) of Delegated Regulation (EU) 2017/565 (investment firms).

↗ The AMC shall establish and maintain an effective compliance function that operates independently and has the responsibility to monitor and, on a regular basis, assess the adequacy and effectiveness of policies, procedures and measures implemented and actions taken to remedy any deficiency in compliance of asset management company and the relevant persons with their professional obligations referred to in II of Article L. 621-15 of the Monetary and Financial Code. Where appropriate and proportionate in view of the nature, scale, complexity and range of their business, AMCs shall establish and maintain an effective internal audit function which is separate and independent from their other

functions and activities and which has the following responsibilities: 1. To establish and maintain an effective audit plan to examine and evaluate the adequacy and effectiveness of the AMC's systems, internal control mechanisms and arrangements; 2. To issue recommendations based on the result of work carried out in accordance with 1°; 3. Verify compliance with those recommendations; 4. Provide reports on periodic control issues – Articles 321-31 and 321-83 of the AMF General Regulation (UCITS), Articles 61(2) and 62 of Delegated Regulation (EU) 231/2013 (AIFs), and Articles 22(2) and 24 of Delegated Regulation (EU) 2017/565 (investment firms).

Good practices:

- Having a specialised outside service provider regularly performing an intrusion test on the AMC's IS in order to: (i) measure the robustness of the cybersecurity system in place and (ii) verify the effectiveness of allowance for the vulnerabilities identified during the previous test.

Bad practices:

- Not defining or monitoring management indicators for maintenance services, IS upgrading and cybersecurity management on the pretext that these services are performed by the AMC's parent Group.
- Deploying the process of permanent/periodic control of sensitive outside IT service providers on the basis of a non-exhaustive list of said providers.