APRIL 2021

SUMMARY OF SPOT INSPECTIONS ON CYBERSECURITY SYSTEMS OF ASSET MANAGEMENT COMPANIES NO. 2 - 2020

amf-france.org

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

INTRODUCTION

As announced in the AMF's supervision priorities for 2020, the second series of SPOT inspections for 2020 targeting asset management companies ("AMCs") consisted of a review of the cybersecurity systems of five companies. This campaign was supplemented by the findings noted during a conventional inspection. The work follows on from the inspections carried out on this topic in 2019.

This further work was justified by the areas of risk identified during the first series of inspections (notably concerning governance of the cyber system and the incident management process), but also by a will to supplement the due diligence conducted by performing technical tests delegated to an accredited external third party.

The inspections were carried out jointly in five AMCs over the period 2017-2020 and enabled us to examine:[1]

□ **Organisation and governance** of the cybersecurity system of the inspected AMCs (internal/external resources, awareness raising among employees, the Information Systems Security ("ISS") strategy, mapping of IT systems and the associated risks, procedural corpus, comitology);

□ **Coordination of IT service providers** by the AMCs (selection, monitoring and evaluation);

□ The cybersecurity **incident management** process (prevention, detection, compilation, analysis, post-mortem, data backup and business continuity);

□ Supervision of the **processes for remote access to the information system ("IS")** of the AMCs (by in-house personnel but also by outside IT service providers and management partners);

□ The **internal control** system in place on cyber risks (organisation, permanent and periodic controls, execution/delegation by the AMC of technical tests on its IS).

The documentary analyses conducted on the coordination of IT service providers were supplemented by the performance of **penetration tests** (“*pentests*”) delegated to an accredited third party selected by the AMF by an invitation to tender. These tests covered outsourced services relating to the IS administration of the inspected AMCs and the supply of their main business application.

The management of cyber risks at the start of the first administrative lockdown decreed in France between 17 March and 11 May 2020 in the context of the Covid-19 pandemic was the subject of a specific analysis. This analysis covered the establishment of the business continuity plan ("BCP"), supervision of the process of remote connection of personnel ("teleworking") and any additional preventive measures taken faced with the risk of a potential upsurge in cyber incidents.

The 2020 campaign of SPOT cyber inspections also used the findings of the conventional inspection carried out in 2020 on the cybersecurity system of a private-equity AMC.

The AMF observes, through this series of SPOT inspections, that the organisation and governance of the AMCs' cybersecurity systems have been reinforced notably through the handling of this subject by a dedicated manager from the executive committee, the implementation of regular awareness raising campaigns for the personnel and the consideration of cyber risks in risk mapping and control plans. **<u>However, based on the principle that only what is well known is well protected, the lack of preliminary work on mapping of the main sensitive data and systems could, despite the efforts made to improve security, allow significant vulnerabilities to persist in the systems inspected, nurturing a false impression of security</u>**. These vulnerabilities concern, in particular, the **insufficient coordination and control of interactions between the AMCs and their third-party service providers**, whether they be IS administrators, application publishers or partners in management operations. Now, the constantly increasing sophistication of the attacks detected by the AMF on the companies supervised reflects hackers' ever-greater

[1] The 2019 SPOT Cybersecurity Summary had covered: organisation and governance of the cybersecurity system, IS administration and supervision, management of sensitive data and business continuity, as well as the cybersecurity internal control system.

knowledge of the data interchange flows between the AMCs and these outside participants, which explains the need for the companies supervised to define clearly beforehand the main assets on which the security improvement efforts should mainly focus.

This overview therefore aims to provide a clarification of the practices of the AMCs under review with regard to the cybersecurity system for their sensitive data, their key processes and their IS in general. This document is neither a position nor a recommendation. The practices identified as either "good" or "poor" highlight approaches identified during the inspections that may facilitate, or hinder, compliance with the regulations.

CONTENTS

1. Reminders 4

2. Summary of the main findings 5

3. Context and scope 7

3.1- Introduction 7

3.2- Presentation of the sample of AMCs inspected 7

3.3- Applicable regulations 8

4. Observations and analyses 9

4.1- Cybersecurity system organisation and governance 9

4.2- Coordination of IT service providers 12

4.3- Cybersecurity incidents management 18

4.4- Supervision of processes for remote access to the IS 24

4.5- Internal control of cyber risks 26

1- REMINDERS

➢ *Definition of cybersecurity risk*

Cybersecurity risk arises from **any potential malicious attack, internal or external, on one of the key features of an AMC's IS**, i.e. its availability, integrity, the confidentiality of the data that it processes, the traceability of the actions that are performed in it by the users and the non-repudiation[2] of these actions. It is customary to summarise these characteristics by the acronym **AICT (Availability, Integrity, Confidentiality, Traceability)**. This 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. The materialisation of this risk can effectively also result in a regulatory non-compliance[3] 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, standby facilities and/or backups are unusable);

□ **appropriate and sufficient resources (IT systems in particular)**;

□ a **robust system for protection of sensitive data** (on investors, collective investment products 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.[4] However, it should be remembered that cybersecurity risk can have an impact on the AMC's compliance with its GDPR obligations.

It should be remembered 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 exceeding 5% of its regulatory capital.*" (Articles 321-35 (UCITS management) and 318-6 (AIF management) of the AMF General Regulation).

➢ Glossary

Term	Definition
IS administration	This is the implementation of all the technical and non-technical measures designed to maintain the operational condition and security of the IS and manage minor/major changes.
Antivirus software	Software capable of detecting and destroying computer viruses.
Strong authentication	Authentication procedure which requires the concatenation of at least two factors: what the user knows (e.g. a password) and what he has (e.g. an authentication token).
Encryption	A cryptography process by which a document can only be deciphered and made understandable by someone who has the encryption key.
The Cloud	The Cloud provides storage space, computing power and executable software in a remote data centre. The word expresses the fact that the server used for this purpose is not directly visible to the user, but hidden as though behind a cloud. A Cloud consists of servers located remotely and accessible from anywhere at any time via a secure, protected internet connection.
Security patch	The security patch is a portion of code added to an existing program after it has been brought into production in order to fix a security flaw.

[2] Ability of the IS to link the actions performed in the IS by a user unambiguously (and without possible dispute) 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.

[3] Refer to the box below on the "main legal rules".

[4] Regulation No. 2016/679 of the European Parliament and of the Council of 27 April 2016, the so-called General Data Protection Regulation (GDPR), is an EU regulation which constitutes the reference document regarding personal data protection. Its provisions have been directly applicable in all 27 EU Member States since 25 May 2018.

Term	Definition
Extranet	This involves the use of a portion of the internet by an organisation to interconnect with its partners. In contrast, an intranet is confined to the organisation's internal network.
IP filtering	Internet Protocol filtering: a security technique designed to restrict access to websites normally accessible on the network.
Firewall	The firewall is software or hardware capable of ensuring compliance with the network security policy, defining what types of communications are authorised on this IT network.
Phishing	Technique used by fraudulent operators to obtain personal information with a view to stealing the identity of an individual or an organisation.
SaaS	Software as a Service: model of commercial software operation. The software is installed on remote servers. Clients do not pay for an operating licence for a version but use the online service for which they pay a subscription fee.
Spam	Unwanted and unsolicited email received in the user's professional mailbox, which may contain links to malware.
Attack surface	This is the sum of the weak points of a system through which an unauthorised user could potentially enter into a software environment and extract data from it.
VPN	Virtual Private Network: system for creating a direct link between remote computers. In particular, allows secure remote access to the corporate network from a mobile terminal.
Wi-Fi	Wireless Fidelity: local area network capable of wirelessly connecting several IT devices.

The good and poor practices identified during inspections (and mentioned below) should be considered in light of the sample of AMCs inspected, namely, for 5 companies out of 6, **independent companies (i.e. not members of a group)**.

2- SUMMARY OF THE MAIN FINDINGS

The trend noted following the first campaign of cybersecurity SPOT inspections (carried out in 2019) is confirmed. In other words, cybersecurity risks are **increasingly well factored into** the governance and control systems of all the AMCs inspected. However, this has been achieved without sufficient prior research on the main risk areas to be protected, which helps maintain a **false impression of security** among the players inspected.

Managers' visibility concerning cyber risks has been bolstered, in all the companies inspected, by the **independence** of the function in charge of IS security management relative to the function of IS Director/Manager. Furthermore, governance is based on the management of cyber risks by a specific executive, who is a member of the Management Committee. Lastly, the personnel are targeted by **regular awareness raising campaigns**, although the performance of periodic phishing tests[5] to measure the development of this awareness remains limited.

On the other hand, reporting to managers (and to internal supervisory bodies such as the board of directors) regarding these risks is seldom organised (2 cases out of 6) in a bespoke committee. The same is true regarding the consideration of these risks in the procedural corpus. For example, although the gradual formalisation of generic security rules is noted (e.g. in the internal charter on the use of IS), formalisation of the cyber strategy pillars remains incomplete due to a **lack of work on the classification and mapping of sensitive data and critical systems** based on the four AICT criteria defined above.

Also, the AMCs of the sample group have formalised a procedure for the **selection and evaluation of IT service providers** which includes a consideration of the level of maturity of the candidates' cybersecurity system. This consideration is also noted in the contracts signed with these service providers, although it proves **superficial in the absence of an audit clause and a procedure for alerting** AMCs in the event of a critical cyber incident.
On the other hand, the processes for evaluation of these service providers remain highly perfectible. First, their implementation is partial because, in the sample group inspected, it concerned only the external IT administrators, and not the business application publishers. Second, their effectiveness is very limited, because they were unable to identify the major vulnerabilities detected via the technical tests of the inspection team (insufficient securing of

[5] Refer to the glossary

the accounts and terminals used for administration, and inefficient management of access rights to sensitive application databases).

In addition, the **cyber incidents** management process was analysed from the viewpoints of (i) the preventive protection of facilities, (ii) the incident compilation and analysis system, and (iii) the process of post-incident business recovery.
Regarding the first point, all the AMCs of the sample group maintain a detailed inventory of their hardware, although **none of them has adopted a policy for managing security components and patches**. The workstations also show classic vulnerabilities (**lack of disk encryption**[6] for 5 out of 6 AMCs, users who are **administrators of their terminal** for only 2 out of 6 AMCs).
Regarding the second point, most of the AMCs (4 out of 6) have established a procedure for managing cyber incidents and all have deployed a database allowing the compilation and analysis of such incidents. Regarding this, the fact that no damage has been caused by the cyber incidents incurred by the AMCs inspected **cannot be considered a guarantee of security**. This is because the feedback on incidents handled by the AMF in 2020 (targeting companies outside the present SPOT campaign) points to ever-more sophisticated approaches (attempts to hijack fund login credentials or to retrieve confidential data) which reflects the patience, meticulousness and growing understanding of the business flows of AMCs by potential attackers.
Lastly, regarding the third point, the inspection team noted the formalisation of a data backup and business continuity plan for the whole sample group. However, most (4 out of 6) of the AMCs inspected do not perform **regular tests on restoring backup data**. As regards the BCP, its coverage remains partial (concerning, for example, the consideration of cyber incidents as the triggering factor), **although the lockdown of the spring of 2020 allowed intensive testing**.

The IS remote access processes of the AMCs of the sample group were also analysed. The access of employees (in the context of teleworking) and external IT administrators is governed by controls for both prevention (identification and specific connection password, encryption of communications) and detection (connection tracing). As regards access by investors, they are confined to portions of the IS isolated from the rest of the network, thereby limiting the risk of contagion. However, the protocols for the exchange of data with the systems of external business partners (e.g. depository, auditor) **are not mapped for 50% of the sample group and are vulnerable** for 2 of the AMCs inspected (given the use of an unsecured communication protocol). Moreover, risk mapping omit these risks for 5 out of 6 AMCs inspected.

Finally, the existing internal control of the cybersecurity system focuses on the coordination of IT service providers and the handling of cyber incidents, but **for 50% of the AMCs inspected it omits the process of sensitive data backup and storage**. It should also be noted that 4 out of 6 AMCs made use of an accredited third-party service provider to perform a pentest on their website or their network.

[6] Refer to the glossary.

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 within 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*).

The European Systemic Risk Board (ESRB) reasserted, in a 2020 report on cyber risk,[7] that the existing high level of interconnection between financial entities, financial markets and financial market infrastructure could constitute a systemic vulnerability. These interconnections can facilitate the spread of localised vulnerabilities through the channels of financial transmission and have negative consequences for the stability of the EU's financial system, resulting in problems of liquidity and a general loss of trust in financial markets. Against this backdrop, on 24 September 2020 the European Commission published the **draft regulation DORA (for *Digital Operational Resilience Act*)** on digital operational resilience in the financial sector, together with a draft directive. This draft regulation plans to make asset management companies obliged entities.

The provisions of the draft DORA regulation define a base of common minimum requirements concerning the establishment of **comprehensive governance and internal control frameworks** for risks related to Information and Communication Technologies ("ICT"), the implementation of a specific process for **management of incidents** related to ICT and the establishment of an **operational resilience test programme**. The draft also defines the key principles for management of the **risk related to IT service providers** and establishes rights and obligations within the framework of the establishment of contractual agreements between financial entities and any IT service provider.

Furthermore, the proposed legislation will allow financial entities to exchange with one another information and intelligence concerning IT threats. Lastly, the draft regulation DORA clarifies the control and enforcement powers of the financial regulatory authorities.

The Association Française de la Gestion Financière (French Asset Management Association AFG) recently published two guides on cybersecurity for AMCs: Cybersecurity in four steps[8] (in October 2019) and a document on data classification and protection[9] (in October 2020).

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 an **independent entrepreneurial company** performing UCITS management and discretionary management and providing an investment advisory service;

□ AMC 2 is also an **independent entrepreneurial company** performing UCITS management and discretionary management;

□ AMC 3, independent since 2000, is specialised in **private equity** and invests in unlisted European companies;

[7] esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html

[8] https://www.afg.asso.fr/wp-content/uploads/2019/10/guide-professionnel-cyberscurit-octobre-2019.pdf

[9] https://www.afg.asso.fr/guide-professionnel-cybersecurite-en/

□ AMC 4, independent since 2004, is specialised in **private equity** and invests in the development of French SMEs;

□ AMC 5 is the fully-owned subsidiary of a listed real estate investment company specialised in commercial property services. It structures and manages long-term **real estate investment** vehicles.

In parallel to the SPOT inspections, in 2020 the AMF also inspected another **independent private equity AMC** (specialised in development capital transactions on medium-sized enterprises)[10] on the topic of cybersecurity. The results of the 'conventional' inspection on this AMC (No. 6) have been included in the findings outlined below for the purpose of comparison with the sample of AMCs inspected within the framework of the SPOT inspections.

The investigations covered the period from 1 January 2017 to 14 December 2020.

3.3- APPLICABLE REGULATIONS

In exercising its prerogatives, the inspection team was supported by the following regulations and policy:

Organisation rules

a) Article 321-23 (I), (II) of the AMF GR (UCITS), Article 318-1 of the AMF GR, Article 57 (1) (a) of Delegated Regulation ("DR") (EU) No. 231/2013 (AIFs) and Article 21 (1) (a) of DR (EU) No. 2017/565 (investment firms) concerning **the appropriate and sufficient material, financial and human resources which the AMC must have, and the establishment and operational maintenance of decision-making procedures and an organisational structure specifying in a clear and documented form the management lines and the breakdown of functions and responsibilities;**

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

c) Article 321-25 of the AMF GR (UCITS), Article 57 (3) of DR (EU) No. 231/2013 (AIFs) and Article 21 (3) of DR (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 and control system

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

e) Articles 321-23 (IV) and 321-31 of the AMF GR (UCITS), Articles 57 (1) (c) and 61 (2) of DR (EU) No. 231/2013 (AIFs) and Articles 21 (1) (c) and 22 (2) of DR (EU) No. 2017/565 (investment firms) concerning **the establishment of an effective compliance function, operating independently, and the establishment and operational maintenance of appropriate internal control mechanisms designed to ensure compliance with the fund manager's decisions and procedures at all levels;**

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

[10] Medium-sized enterprises

g) AMF Position-Recommendation 2014-06 **(Guide to the organisation of the risk management system of AMCs);**

Responsibility of senior management

h) Article 321-35 (g) of the AMF GR (UCITS), Articles 318-6 of the AMF GR and 13 (2) of DR (EU) No. 231/2013 (AIFs) concerning **incident compilation and associated notification of managers and the AMF**;

i) Articles 321-35 and 321-36 of the AMF GR (UCITS), Article 60 (1), (3), (4) and (6) of DR (EU) No. 231/2013 (AIFs) and Article 25 of DR (EU) No. 2017/565 (investment firms) concerning **executives and internal supervisory bodies accountability as well as reports communicated to these bodies concerning compliance, risk control and periodic inspection;**

Outsourcing

j) Articles 321-93 to 321-96 of the AMF GR (UCITS), Articles 318-58 to 318-61 of the AMF GR (AIFs), Article L.533-10 II 4° of the Monetary and Financial Code and Articles 30 (1) and 31 of DR (EU) No. 2017/565 (investment firms) concerning **the outsourcing of essential or important tasks or operational functions;**

Data recording and retention

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

l) 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;**

m) Articles 321-69 to 321-74 of the AMF GR (UCITS), Articles 57 (1), 58 and 64 to 66 of DR (EU) No. 231/2013 (AIFs) and Article 312-41 of the AMF GR and Article 75 of DR (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

4.1- CYBERSECURITY SYSTEM ORGANISATION AND GOVERNANCE

➢ *Organisation and human resources of the AMC's cybersecurity system*

All the AMCs inspected have established an **internal** IT function:

- AMCs 1, 2 and 6 have an Information Systems Manager ("ISM");
- AMCs 3 and 4 have assigned the IS supervision activity to an executive manager performing other duties (Finance Director for AMC 3, Company Secretary for AMC 4);
- AMC 5 is managed by the Chief Information Officer ("CIO") of its parent Group (noting that this AMC has no in-house system and uses all the applications and facilities of its parent company).

On the other hand, the responsibility for ISS is **insourced** for only half of the companies inspected, i.e. AMCs 2, 5 and 6 for which it forms part of the duties of the ISM/CIO. For AMCs 1, 3 and 4, this function has been delegated to the third-party service provider that is also in charge of IS administration.

Within this framework, the function of Chief Information Security Officer ("CISO") is **independent** for all the sample group inspected. In particular:

- For AMCs 1, 3 and 4, the ISS activities performed by the external administrator are supervised by a member of the Executive Committee reporting directly to one of the senior managers of the AMC;
- For AMC 2, these activities, performed by the in-house ISM, are supervised by one of the managing directors ("MDs") of the AMC;
- For AMC 5, these activities, performed by the Group CIO, are supervised by the chairman of the Management Board of the AMC, in charge of cyber risk management;
- For AMC 6, these activities, performed by the in-house ISM, are supervised by the Chief Digital Officer who reports to the AMC's senior managers.

As regards the resources invested to maintain this organisation, they remain proportional to the amount of assets under management, as shown, for example, by the following table for financial year 2019 (the assets under management and net earnings are given to provide a basis for comparison).

AMC No.	**1**	**2**	**3**	**4**	**5**	**6**
AUM (€m)	500	565	785	**505**	**1,600**	**2,267**
Net earnings (€m)	1.29	0.39	9.7	2	10.9	5.9
IT budget (€k)	260	260	134	154	569	969
Cyber budget (€k)	**Inseparable from the IT budget**			4.8	42	223
% cyber/IT budget	N/A			**3%**	**7%**	**23%**

➢ *Governance of cybersecurity risk in the AMC*

Subjects relating to cybersecurity are represented by a specific contact person **in the management body** of each of the AMCs inspected. This is:

- For AMCs 1 and 4: the Company Secretary in charge of supervising the external IT administrator;
- For AMC 2: one of the MDs in charge of IT issues;
- For AMC 3: the Finance Director in charge of supervising the external administrator;
- For AMC 5: the chairman of the AMC's Management Board specifically in charge of management of this risk and reporting to the Group CIO;
- For AMC 6: the Chief Digital Officer, a member of the Executive Committee, to whom the ISM reports.

On the other hand, the management of cybersecurity issues is the subject of a specific regular committee meeting for only the 2 AMCs with the largest assets under management (AMCs 5 and 6). For the other four AMCs, monitoring of cyber risk developments **is not included in the existing committee meetings**, including the Risks Committee.

Regarding the **procedural corpus** of the AMCs inspected, it addresses cybersecurity rules:

- specifically for AMCs 2, 4, 5 and 6, via an appropriate procedure or a specific section of the risk management procedure;
- generically for AMCs 1 and 3, through the expression of good practices concerning the use of the company's IT facilities, set out formally in the internal rules or the IT charter.

However, only 2 of the 6 AMCs (No. 4 and 6) have formalised a clear cybersecurity strategy (stressing the security measures taken with regard to the main identified risk areas) in a **general security policy**.

➢ *Preliminary identification of sensitive data and systems*

Only AMC 2 has a policy of data classification according to their level of criticality and mapping of its sensitive data. For **the other AMCs, this work is non-existent (AMCs 3 and 6) or partial. More specifically:**

- AMC 1 has not established a data classification policy but has defined the main families of data with which it works (for example, fees, reporting) and has begun to formalise the existing data flows with its partners in management operations (the depository in particular);

- AMC 4 has not established a data classification policy but has formalised a map of in-house electronic data processing operations using personal data;
- AMC 5 has not established a data classification policy but has begun to formalise the storage areas and formats for the main families of business data that it has identified.

Likewise, **only 2 of the 6 AMCs inspected (AMCs 1 and 2) have mapped their sensitive IT systems.**

Accordingly, only the cyber approach of AMC 2 is based on a detailed and pre-emptive analysis of the areas of major risks incurred by its sensitive data and systems. For the other five AMCs, the non-existent or partial nature of this essential preliminary work entails a twofold risk: first, the risk of non-exhaustive coverage of the most critical IS portions, and second, the risk of a cyber approach omitting one or more of the four AICT pillars constituting a sustainable cyber approach.

➢ *Consideration of cyber risks in risk mapping*

Unlike for data and systems mapping, **risk mapping of the six AMCs inspected take into consideration cyber risks**, especially in the case of AMCs 3 and 6 which have taken care to define the potential impacts on all their operating processes. This work is still in progress for the other four AMCs given that:

- for AMCs 1 and 2, the current risk mapping omits the risk of breaches of data **confidentiality and integrity**; and
- for AMCs 4 and 5, it omits the risks due to **the processes of remote access** to its IS.

➢ *Raising the AMC personnel's awareness of cyber risks*

Employee awareness raising programmes have been established in the six AMCs of the sample. These programmes take the form of in-person learning (for AMCs 1, 3 and 6), an awareness raising kit handed to newcomers (AMCs 2 and 3), the sending of newsletters to employees (for AMCs 3, 4 and 6) and the posting of security information on the enterprise social network (for AMC 5).

On the other hand, **only AMC 5 has tested in real-world conditions the level of its employees' awareness** of cyber risks. This test took the form of participation in a phishing test carried out in November 2019 on the personnel of its parent company. The awareness raising measures performed, post-test, by the CIO on employees needing this proved successful, because (real) phishing attacks occurring in H1 2020 were stopped as soon as they were identified by the employees.

Regulatory reminders:

- ↗ 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(1) (b) of Delegated Regulation (EU) No. 231/2013 (AIFs), and Article 21 (1) (b) and d) of Delegated Regulation No. 2017/565 (investment firms).
- ↗ 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 GR (UCITS), Articles 318-4 of the AMF GR and 61 (1) of DR (EU) No. 231/2013 (AIFs), and Articles 312-1 of the AMF GR and 22 (1) of DR (EU) No. 2017/565 (investment firms).
- ↗ Executives and, if need be, internal supervisory body, are accountable of AMCs' compliance to their professional obligations. They periodically assess and control efficiency of policies, systems and procedures set up to ensure compliance, and take any needed measures to remediate potential defects. Executives shall receive at least once a year, reports on compliance, risk control and

periodic control. These documents shall notably reports measures taken to remediate potential defects. Internal supervisory bodies, if they are in place, shall be included into the distribution list of these type of reports (Articles 321-35 and 321-36 of the AMF GR (UCITS), Article 60 (1), (3), (4) and (6) of DR (EU) No. 231/2013 (AIFs) and Article 25 (2) of DR (EU) No. 2017/565 (investment firms).

- AMCs shall periodically map their risk of non-compliance. This mapping should enable them to set the targets, resources and work programme of the compliance function. The work programme and resources of the compliance function should be reviewed regularly to take into consideration, where applicable, any emerging risk resulting, for example, from the launch of a new business (AMF Position-Recommendation 2014-06).

Good practices:

- Ensuring the independence of the CISO function in relation to the CIO (and the visibility of cyber risks) via (line or staff) reporting by this function to the Executive Committee.[11]
- Targeting the cyber risk awareness raising effort on employees needing it most, identified through the results of regular phishing tests.
- In the AMC's annual budget and IT spending, singling out spending on cybersecurity.[12]

Poor practices:

- Not including the monitoring of cyber risks in the periodic risks steering committee (which involves senior manager of the AMCs), nor in the regular reporting distributed to executive committee and internal supervisory body (for example: board of directors, supervisory board).
- Limiting Information Systems Security procedures to a list of generic principles without endeavouring to formally explain the measures taken, as part of a cyber strategy, with regard to the main identified risk areas.
- Deploying a cybersecurity system without (i) prior identification, (ii) classification by level of criticality (based on the AICT criteria) and (iii) a regular review of sensitive data and IT systems.[13]

4.2- COORDINATION OF IT SERVICE PROVIDERS

Formal framework for selection and evaluation of IT service providers

All the AMCs in the sample, **except AMC 2**, have established a procedure for selection and evaluation of IT service providers. All these procedures include consideration of the quality of the cybersecurity system of the service providers targeted within the framework of services rendered, **except for AMC 5**.

In order to verify the correct execution of these procedures, for each member of the sample group inspected, the team selected two outside IT service providers, whose services rendered to the AMCs prove sensitive.

AMC No.	1	2	3	4	5	6
Activity	UCITS management/investment firm		Private equity		Real estate management	Private equity

[11] Good practice already identified during the 2019 Cyber SPOT campaign.

[12] Good practice already identified during the 2019 Cyber SPOT campaign.

[13] Poor practice already identified during the 2019 Cyber SPOT campaign.

First service provider selected	External IT administrator	N/A[14]	Same as for AMC 1			Publisher of the application for management of commercial contacts and tracking of equity investments
First service provider selected	Publisher of the discretionary management application	Publisher of the depository application	N/A[15]	Publisher of the equity investment management application	Publisher of the real estate management application	Publisher of the virtual space for sharing with investors

Regarding the external IT administrator: the existence of a contract binding AMCs 1, 3, 4 and 5 to their respective external IT administrators was observed. These contracts list the IT services supervised by the service provider. However, they do not indicate the cybersecurity measures demanded of the service provider when performing its due diligence for AMCs 3 and 4. Moreover, **none of these contracts clearly specifies the protocol for alerting the AMCs if the service provider detects a cyber incident, or includes an audit clause.**[16]
However, the external IT administrators of the test sample **underwent evaluations by the AMCs inspected**. These evaluations took the following forms:

- For AMC 1: oral discussions during regular meetings of users of the application (which are not covered by formal minutes);
- For AMCs 3 and 4: evaluation reports in 2019 and 2020;
- For AMC 5: formal reviews in 2018 and 2019.

Regarding the publisher of the main business application: the existence of a contract binding AMCs 1, 2, 4, 5 and 6 to the publisher was observed but **none of these contracts includes an audit clause**.

Unlike what was noted for the external IT administrators, **AMCs 1, 2, 4, 5 and 6 have not established a process for regular formal evaluation of the services rendered by the publisher of their main business application**. More specifically:

- AMC 1 has not formalised an evaluation report for this service provider. Moreover, the minutes of service follow-up meetings conducted with the service provider do not address cyber risks;
- AMC 2 has not formalised such an evaluation system;
- AMCs 4 and 6 have formalised such a system, but have not applied it to the publisher of their main business application (nor to the publishers of the other IT applications used);
- AMC 5 formalised a single evaluation of the publisher of its main business application unit in 2019, but without covering this service provider's management of cyber risks.

➢ ***Technical tests performed on the main outsourced IT services***

In order to measure the quality of the cybersecurity system established by the AMCs inspected for the IT services that they have outsourced, technical tests were carried out by the inspection team. The scope of these tests covered the services identified as sensitive in the above table (section 4.2).

[14] IS administration for AMC 2 is performed by the ISM. This function is also insourced for AMC 6.

[15] AMC 3 does not use business applications.

[16] Such a clause would allow the AMC to perform an audit (or delegate the performance of an audit) on the cybersecurity level of the service provided.

The operational performance of technical due diligence was entrusted by the inspection team to an Information Systems Security Audit Service Provider ("**PASSI**") accredited by French National Cybersecurity Agency **ANSSI** and selected beforehand by tendering. The work of the "PASSI" involved a team of seven consultants.[17] The work took place **from 1 October to 8 December 2020.**[18] Each operation was covered by a test agreement signed by the AMF, the "PASSI" and the AMC inspected. The approval of a fourth participant (the publisher of the tested applications) by signature of the agreement was necessary for AMCs 2, 3 and 6. This is because, for these three AMCs, the tested applications are provided in SaaS mode,[19] i.e. they are hosted on the IT systems of the publisher, and not directly on those of the AMC.[20] The publisher's approval therefore proved necessary to allow the work of the "PASSI" on an IS of which it is ultimately the owner.

The tests carried out were **completely transparent** with regard to the AMCs of the sample group and their respective IT service providers. **The time slots, scope, objectives and technical targets of the tests were defined beforehand** and set out formally in signed agreements. Any business constraints for the AMCs were thus able to be allowed for before starting the due diligence.

To allow homogeneous work to be performed on all the companies inspected in a limited time, **the objectives of the "PASSI" tests were determined from the outset**. These objectives were as follows:

- Assess the level of maturity of the external IT administrator in light of the **main recommendations of the secure IS administration guide**[21] **published by ANSSI**;
- Assess the level of maturity of the cybersecurity system for the main business applications relating to the risks of **data theft** (client data in particular) and of **an unauthorised user taking control of the application's functionalities (in-house or remotely)**.

The results obtained after carrying out the technical tests were the subject of a feedback meeting with each of the AMCs concerned.[22] The proven vulnerabilities are described below.

Identified vulnerabilities concerning the services rendered by the external IT administrator

Reminder: AMCs 2 and 6 are not included in the following table because the administration activities of their respective IS's are not outsourced.

Identified vulnerability[23]	Associated risk	AMC concerned by the identified vulnerability			
		No. 1	No. 3	No. 4	No.5
The external IT administrator **does not use a terminal dedicated to his IS administration activities**. The terminal used is connected to the internet and its USB ports are not blocked.	**Contamination** of the administrator's terminal leading to contamination of the AMC's network	Yes	Yes	Yes	No
Administration of terminals and servers is performed through a **single generic administrator account.**	Extended access to the AMC's IS in the event of **identity theft** affecting the administrator account	Yes	No	Yes	Yes

[17] These consultants performed work in accordance with Article L. 621-9-2 2° of the Monetary and Financial Code which stipulates that: "*The Autorité des Marchés Financiers may: […] 2° Have recourse, for its inspections […] to […] competent individuals.[…]* ". All those involved in the work were provided with a personal engagement letter.

[18] Except for AMC 6: see "special case" section below

[19] Refer to the glossary.

[20] Unlike AMCs 1 and 5 for which the tested application was hosted directly by the companies inspected.

[21] Available at: https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/

[22] Only AMC 3 was accompanied by its external IT administrator at the feedback meeting.

[23] These vulnerabilities are listed in decreasing order of the potential level of impact.

Identified vulnerability[23]	Associated risk	AMC concerned by the identified vulnerability			
		No. 1	No. 3	No. 4	No.5
The administration interface used by the external administrator to perform his operations on the AMC's IS is **visible from the internet.**	Easier for an external attacker to **take over control** of the AMC's IS	Yes	No	No	No
The AMC's external IT administrator is a company owned by a sole shareholder: the manager and sole employee has **no replacement/substitute** to perform his duties.	Risk of occasional unavailability, or even **failing**, of the external IT administrator in his IS administration duties for the AMC	Yes	No	No	No

<u>Identified vulnerabilities concerning the services rendered by the business applications publishers</u>

<u>Reminder:</u> AMCs 3 and 6 are not included in the following table because AMC 3 does not use a business application (apart from the Microsoft Office software suite).
The vulnerabilities identified following the technical tests performed on the IS of AMC 6 are shown in a specific table in the following section.

The tests were conducted in the target-application production environment. Regarding this, no attack designed to cause a **temporary blockage** of one of the tested components[24] was performed. Moreover, no psychological manipulation technique for the purpose of obtaining useful information compromising the targeted systems was used.[25]

Identified vulnerability[26]	Associated risk	AMC concerned by the identified vulnerability			
		No. 1 (UCITS/mandates)	No. 2 (UCITS/mandates)	No 4 (private equity)	No. 5 (real estate)
Recap of the role of the tested application		Discretionary management	Depository application	Equity investment management	Real estate invest. management
Data extractions from the application are neither technically limited nor traced.	No early detection of **massive data leaks**	Yes	No	No	Yes
The application's **database protection** system is inadequate.	**Loss of integrity/confidentiality** of the application database	Yes: the flow allowing the application to contact its database **is not encrypted.**	**Yes: the terminal for administration of the application login portal can be used to read/modify the database**	No	Yes: the flow allowing the application to contact its database **is not encrypted.**
The **technical restrictions on modification of the tables for management** of access rights to the application's database are	**Unauthorised access to sensitive data** by an in-house user having escalated his privileges in the application	Yes	No	**Yes: the vulnerability is exacerbated by the application's insufficient level of**	Yes

[24] So-called "denial of service" attacks.

[25] So-called "social engineering" technique

[26] These vulnerabilities are listed in decreasing order of the potential level of impact.

Identified vulnerability[26]	Associated risk	AMC concerned by the identified vulnerability			
		No. 1 (UCITS/mandates)	No. 2 (UCITS/mandates)	No 4 (private equity)	No. 5 (real estate)
Recap of the role of the tested application		Discretionary management	Depository application	Equity investment management	Real estate invest. management
inadequate, or even non-existent.[27]				**automatic checking of users' identity and rights when logging in**	
The process of management of access rights to the application is **not expressed formally**.	*Same as above*	Yes	No	Yes	No
The application's administration interface is **shown on the web**, including outside the AMC's network.	**Significant increase in the attack surface**[28] of the application	No	No	**Yes:** The **lack of IP filtering**[29] adds extra vulnerability residing in the lack of automatic blocking, by the application, of login attempts coming from unauthorised sources.	No

The critical vulnerabilities indicated in red in the above table were, upon detection by the "PASSI", reported via a security alert to the application publisher for immediate remediation.

Special case: vulnerabilities identified in the course of tests performed on AMC 6

AMC 6 was the subject of a separate approach from the other five AMCs of the sample group, through a conventional inspection which took place from 4 November 2019 to 28 July 2020. The timeline for performance of the technical tests (20 February - 2 July 2020) was **impacted by the administrative lockdown** decreed by the French government between 17 March and 11 May 2020. In particular, AMC 6 did not want its IS to be targeted by external tests over this period of intensive solicitation post-implementation of the BCP.[30]

On completion of this work, and given the security measures adopted by AMC 6 and the respective publishers of the two applications tested, the ability of an attacker to harm them without having a terminal and a user account of the AMC was estimated as **practically nil, which correspondingly reduces the likelihood of occurrence of such an attack.** On the other hand, four vulnerabilities were identified by the "PASSI" in the immediate IT environment of the tested applications. Their potential impact is significant, because it relates to the potential disclosure of

[27] This means that an authenticated user is able to escalate his privileges so as to become an administrator.

[28] Refer to the glossary.

[29] Refer to the glossary.

[30] All the personnel of AMC 6 having been placed in teleworking during the lockdown period mentioned.

information that is confidential for the AMC. However, their probability of occurrence is considered low, because, to be exploited, all require the physical presence of the attacker **on the premises of the AMC**.

Identified vulnerability[31]	Associated risk
It is possible to access the administration interface of the AMC's shared multifunction printer without using a password. It is also possible to configure thereon an email address which will receive a copy of any document recorded by the copier.	Fraudulent retrieval of the documents recorded by printers (by an attacker having access to the copier).
It was possible to access in read mode a **network share** (user-created) containing work files including sensitive data. This share was[32] accessible to everyone without any restriction on user profiles.	Retrieval of files available on the user-created network shares by an attacker having access to the internal network of AMC 6.
It is possible to map the information system of AMC 6 without prior authentication by logging in to the network dedicated to **videoconferencing.**	Retrieval of information on the network (by an attacker present on the premises of AMC 6) in order to prepare a cyberattack.
The **Google Chrome browsers** on the terminals of AMC 6 authorise installation, by the users, of browser extensions without any restriction.	Installation, by a relatively unsophisticated user, of browser extensions that could contain spyware.

The test reports produced by the "PASSIs" were attached to the inspection reports sent to each AMC as a **guide for remediation by their service providers**. Regarding AMC 6, the tests having been carried out in cooperation with the ISM, the remediation plan was initiated upon completion of their formalisation.

Regulatory reminders:

- 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 – Article 321-24 of the AMF GR (UCITS), Article 57 (2) of DR (EU) No. 231/2013 (AIFs), and Article 21 (2) of DR (EU) No. 2017/565 (investment firms).
- If AMCs outsource the execution of operational tasks and functions that are critical or 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 – Article 321-93 of the AMF GR (UCITS), Article 318-58 of the AMF GR (AIFs), and Article L. 533-10 II 4° of the Monetary and Financial Code (investment firms).
- AMCs shall exercise due skill, care and diligence when entering into, managing or terminating an outsourcing contract for critical or important operational tasks or functions. In particular, AMCs must take the necessary steps to ensure that the following conditions are satisfied: The service provider must carry out the outsourced services effectively. For this purpose, AMCs shall define methods for evaluating the service provider's level of performance; the service provider must properly supervise the performance of outsourced tasks or functions, and adequately manage the risks stemming from outsourcing; 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; AMCs and the competent authorities shall have effective access to the data relating to the outsourced tasks or functions; the service provider must protect any confidential information relating to the AMC and its clients; the AMC and the service provider must establish and maintain an effective contingency plan for disaster recovery and providing for periodic testing of backup facilities, wherever that appears necessary given the nature of the outsourced task or function – Article 321-96 II (2), (3), (5), (9), (10), (11) of the AMF

[31] These vulnerabilities are listed in decreasing order of the potential level of impact.

[32] This vulnerability was resolved during the test by the ISM of AMC 6.

GR (UCITS), Article 318-61 II (2), (3), (5), (9), (10), (11) of the AMF GR (AIFs), and Article 31 (2) (b) (c) (e) (i) (j) (k) of DR (EU) No. 2017/565 (investment firms).

Good practice:

- Establishing a procedure for selection and regular evaluation of IT service providers taking into consideration the cyber risks involved in their activity.

In line with this good practice, the AMF expected to note equally the following good practices:

- Ensuring implementation, by the **external IT administrator**, of measures to secure his operations on the AMC's IS (workstations dedicated to the administration activity, nominal administrator accounts, existence of a substitute in case of absence of the principal administrator).
- Ensuring implementation, by the **external IT administrator**, of security measures restricting access to (i) copier administration interfaces and (ii) videoconferencing networks only to authorised users.
- Ensuring the gradual restriction, or even elimination, of the level of internet visibility of the **external administration** interfaces on systems and applications.
- Ensuring implementation, by the **application publishers**, of the necessary measures for secure use of sensitive applications (restriction of data extraction, precise formal management of access rights to applications and the associated databases, encryption of database access).
- Performing, at least once a year, an evaluation of the cybersecurity level of services rendered by the **application publishers** (development, advice, support), notably through participation in user meetings, the organisation of service steering committees and/or regular requests for reports on the security audits conducted by the service provider on its own systems.

The inspection team rather observed the following poor practices in this field.

Poor practices:

- Failing to include an audit clause in contracts binding the AMC to its IT service providers.
- Not stating in contracts binding the AMC to an **external IT administrator** (i) the cybersecurity measures required of the administrator in performing his activities and (ii) the emergency protocol for notification of the AMC if the administrator detects a cyber incident that could affect the AMC.

4.3- CYBERSECURITY INCIDENT MANAGEMENT

➢ ***Technical measures for the prevention of cybersecurity incidents***

None of the six AMCs inspected has formally expressed a policy for management of IS components[33] and security patches.[34] On the other hand, all have established an inventory of the hardware and software components of their IS. In addition to tracking versions of each software program (to regularly check the homogeneity of the installed IT resources), this inventory makes it possible to clearly identify the hardware not currently allocated. Finally, the date of the last update of these inventories is recent (H1 2020). However, **the inventory of AMC 4 is still underway** because the personnel to whom the workstations are allocated are not indicated.

To complete the analysis of the cyber incident prevention system of each AMC of the sample group, the team carried out a documentary review of the existing security systems on the main components of the IS, namely the

[33] Hardware and software.

[34] Refer to the glossary. The absence of such a policy entails, in particular, a risk of heterogeneity in the security level of the various IS components, conducive to the creation of vulnerabilities that could be exploited by a pirate.

network, Wi-Fi,[35] (local)[36] servers, workstations, mobile devices[37] and email service. The results of this review are set out formally in the following table (the vulnerabilities detected in this context are shown **in red**).

Scope	AMC					
	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6
Network	Internet access protected by a firewall. Real-time traffic monitoring.					
	User access is subject to strong authentication by an ID and password.	Same as for AMC 1 **but the password security criteria for logging in to this network are not sufficiently robust in light of the ANSSI's recommendations**[38]	Same as for AMC 1			
Wi-Fi	Employee access protected by password. "Guest" access not allowing connection to the AMC's network.					
Local servers	Secure physical access. Antivirus protection.		N/A	Same as for AMC 1		
Workstations	Protection by antivirus software/antispyware. Homogeneity of installed software versions.					
	The users are administrators of their workstations.[39]	N/A			**Same as for AMC 1**	N/A
	The workstations are not encrypted.[40]					N/A
Mobile devices	Centralised administration allowing remote deletion of the data in case of theft.					
Electronic mail	Firewall filtering all incoming emails "Anti-spam" solution capable of isolating unwanted incoming emails.					

➢ ***Cyber incident management procedure***

AMCs 1, 3, 5 and 6 have **set out formally a cyber incident management procedure** including the processes of reporting, feedback, data input to the dedicated compilation database and description of the system for management of the identified risks by a specific committee. AMC 4 has set out these processes formally in the contract binding it to its external IT administrator. As regards AMC 2, it has not formalised such a procedure.
On the other hand, **all the AMCs of the sample group have set up a database for compilation** of cyber incidents or established a system of identification of these specific incidents in their database of operating incidents.[41]

The analysis of cyber incidents compiled over the inspection period shows the following **trends**.

[35] Refer to the glossary.

[36] This means that only the servers located physically on the premises of the AMC were included in the analysis. Management of the servers kept outside these premises by the IT administrator was dealt with in the preceding part of this summary devolved to the coordination of IT service providers.

[37] Laptop computers, professional mobile phones and tablets.

[38] https://www.ssi.gouv.fr/guide/mot-de-passe/

[39] This entails a risk of the user-administrator downloading a malicious software program to their terminal.

[40] This entails a risk of access to the terminal's data by a hacker after a theft or loss of hardware.

[41] A cyber incident is distinguished from an IT incident (e.g. a fault) in that it is triggered by an intention to harm the target.

AMC No.	1	2	3	4	5	6
AUM (€m)	500	565	785	505	1,600	2,267
Number of **operating** incidents	16	40	756	NS[42]	67	9
Number of **IT** incidents	3	18	NS	101	1	0
Number of **cyber**[43] incidents (% cyber/operating incidents)	0 **(0%)**	3 **(7.5%)**	12 **(1.6%)**	3 **(-)**	11 **(16.4%)**	6 **(66.7%)**

➢ ***Types of cyber incidents detected***

Although the inspected AMCs did not report a notable increase in cyberattacks incurred during the lockdown period, the cyber incidents reported to the AMF in 2020 testify to hackers' growing interest in the asset management sector and their deep understanding of the business flows taking place between AMCs and their partners, as illustrated by the increasing sophistication of attacks. Three categories of such incidents were observed:

- Attempts to **hijack personal credentials** (*phishing*);[44]
- Attempts to **hijack funds;**
- Attempts to retrieve **personal, commercial or strategic data.**

✓ Attempt to hijack personal credentials

The aim of the attackers is to obtain the credentials (ID and password) of targeted employees to be able to access their data, steal their identity in relations with other organisations and replicate this scenario on other targets. The operating procedure observed is as follows:

- The business email account (mailbox) of a key employee of the AMC is compromised by discovering their login and password. For this first step, a simple identity spoofing by the attacker was also observed via the creation of an email address that is fraudulent but contains a domain name visually similar to the original;[45]
- An email message is then sent to the victim's contacts to warn them of information that could generate a strong interest. This message prompts the victim to consult a website or a document containing malicious hypertext links, which is the medium for the attempt to obtain the victims' credentials;
- After compromising the email account of the initial victim, the attacker saves a rule for automatic transfer of the messages sent/received from this mailbox to a pirated mailbox.

This scenario impacted AMC 6 in August 2019 (all the contacts of the initial victim having received the fraudulent email).

The materialisation of this scenario had a serious impact on the AMC's image. After discovering the attack, the victim has to warn all their contacts. Moreover, the repetition of this type of attack on a given target may result in the AMC's domain name being blacklisted by anti-spam service providers.

Regarding remediation, one commonly applied measure is a change of password of the victim whose identity was initially stolen. This action is necessary but not sufficient, because the attacker could potentially have compromised other accounts than the one suffering the identity spoofing. It is therefore advisable for it to be supplemented in

[42] Not specified: the IT incidents and cyber incidents detected by AMC 4 are compiled in a dedicated servicing operation request facility maintained by the AMC's external IT administrator.

[43] According to the classification of each of the AMCs inspected.

[44] Refer to the glossary.

[45] For example, the original email address "first name.family name@ABCD_finances.fr" (for which the domain name is "ABCD_finances.fr") can be imitated by creating the fraudulent email address "first name.family name@ABCD-finances.fr"

particular by **the activation of a strong authentication mechanism,**[46] **a comprehensive review of the rules on email accounts (to identify illegitimate automatic transfer rules) and the deployment of technical mechanisms to verify the authenticity of messages/domain names.**[47]

✓ Attempt to hijack funds (business email compromise, or CEO scam)

This scenario starts like the previous one by compromising the email account of a manager. The aim is to send to an empowered employee of the AMC a request for funds transfer to an external bank account by pretexting an imminent and/or secret deal.

The technical measures for prevention/remediation of this type of attack are similar to those described in the box above. It is important to supplement them by implementing a confirmation call process designed to formally verify any request with one or more identified accredited contacts apart from the request itself (particularly when the destination bank account is unknown, or announced as being recently updated).

✓ Attempt to hijack funds (client scam)

This scenario is similar to the previous one. The attacker steals the identity of an investor who is a client of the AMC, demanding a bank transfer from the AMC. The measures for prevention and remediation of this category of attack are the same as those described in the box above.

The CEO and client scam scenarios impacted AMC 2 (demand for funds transfers made following hacking of the mailbox of one of the managing directors, then those of two clients) and AMC 6 (attempted hacking of the founder's mailbox). No loss was recorded by the AMCs following these attacks, which were uncovered in time.

✓ Attempt to hijack funds (depository scam)

This scenario is more complex than the previous ones because it involves several players: the AMC (a collateral casualty in terms of image), the depository of the funds and the fund investors.

This scenario impacted AMC 6 and one of its depositories, without any loss for the AMC. However, it shows a greater degree of sophistication of the hackers in preparation of the attacks.

The scenario deployed is as follows:

- Step 1: **Attempts made on all fronts to compromise the mailboxes** of the AMC's 38 employees, on all hierarchic levels combined;
- Step 2: Once the mailbox of a company executive has been penetrated, a rule is put in place on this mailbox to **systematically copy incoming/outgoing emails** to the hacker's mailbox;
- Step 3: **Phase of observation and intelligence lasting three months** (April–June 2018) allowing the hacker to collect the business contacts of the hacked executive and understand the functioning of the AMC's business flows in which he takes part;
- Step 4: **Impersonation of a business contact** of the executive mentioned (in this case, the identity stolen was that of an employee of the depository of AMC 6) to ask by an email two fundholders of one of the managed funds **to direct payment of the next call for funds to a fraudulent IBAN**.

This incident had no negative consequences either for AMC 6 or the managed funds, because the two fundholders mentioned made a confirmation call. The mailbox identity thefts or attempted identity thefts suffered gave rise to an audit of the connection logs (to determine the actions carried out with the spoofed account) and an immediate change of login IDs of the user whose mailbox was compromised. In addition, a security audit was carried out by AMC 6.

✓ Attempt to hijack funds (custody account keeper scam)

[46] Refer to the glossary.

[47] Refer to rule 24 of the ANSSI health guide (https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/)

This scenario involves the AMC whose identity is stolen, one of the AMC's clients and the custody account-keeper who is the ultimate target. After compromising the email account of a key employee of an AMC, the attacker creates a domain name visually similar to that of the AMC and sends the custody account-keeper a request for a bank transfer to a fraudulent IBAN presented as being that of a client of the AMC.

This scam scenario impacted AMC 1 post-inspection and its account-keeper. It gave rise to a fraudulent transfer of €220,000 made by the custody account-keeper to the IBAN provided by the hacker.

✓ Attempt to retrieve sensitive data

This category of attack, not specific to AMCs, can take the form of, for example:

- intrusion in application code repositories (such as an extranet),[48] in order to identify vulnerabilities in those codes, to exploit them later;
- intrusion in cloud infrastructures, e.g. by retrieving service technical IDs, containing targeted data.

Potential goals for the attacker include attempted financial extortion from the AMC or its clients, identity spoofing, sabotage, resale of data, or economic espionage.

This scam scenario impacted one AMC outside the scope of the 2020 SPOT campaign, and the hosting service for its IT infrastructure. It resulted in the theft of several thousand items of sensitive data relating to users, clients, potential clients and partners of the AMC.

To protect itself from the negative consequences of incidents of this type, AMC 6 has taken out a **specific insurance policy against cyber risks**. This is not the case for AMCs 1 to 5. On the other hand, the **civil liability** insurance policy of AMC 5 provides it with a guarantee of "*repayment of the necessary costs or restoration in the event of […] destruction […] of the electronic media […] containing information […] belonging to the insured […]*".

➢ *Business continuity arrangements in the event of critical cyber incidents*

All the AMCs of the sample group have **formally defined a business continuity plan** ("BCP"). This plan **takes cyber risks into consideration as a possible triggering factor** for AMCs 2, 4, 5 and 6. This consideration remains partial for AMC 2, for which only a possible firewall flaw/outage is considered a triggering factor, which is simplistic given the diversity of attacks that could target the AMC. As regards AMC 3, it does not take cyber risks into consideration in its BCP.

The business continuity strategies in place in each of the AMCs inspected are set out in the following table (the vulnerabilities identified by the inspection team are shown there in **red**).

BCP	AMC 1	AMC 2	AMC 3	AMC 4	AMC 5	AMC 6
BCP management	Management Committee		Crisis management unit (senior managers, CICO, external IT administrator)			
Continuity strategy in the event of **unavailability of the premises**	Teleworking and/or transfer of personnel to rented offices	Teleworking		Teleworking or transfer of personnel to another group facility		Teleworking
Formal definition of a clear continuity strategy in the event of a **prolonged**	**No**				Yes	

[48] Refer to the glossary.

BCP	AMC 1	AMC 2	AMC 3	AMC 4	AMC 5	AMC 6
telephone outage						
Formal definition of a clear continuity strategy in the event of a **prolonged IS outage**	Yes: restoration of backup data performed by the external IT administrator (for AMCs 1, 3, 4 and 5) or the ISM (for AMCs 2 and 6)					
Formal definition of a clear continuity strategy in the event of **prolonged unavailability of a key person**	**No**	Yes	Yes **but the proposed strategy omits the CIO**	**No**	Yes **but the proposed strategy omits the CIO**	Yes

Each AMC of the sample group has **formalised a plan for regular safeguarding of its data**, but the plan of AMC 2 remains embryonic because it does not include the scope and frequency of the backups made. On the other hand, except for those AMCs having the biggest resources (AMCs 5 and 6), **the companies inspected have not implemented regular restoration tests on backup data**. These tests are non-existent for AMCs 2 and 3 and partial for AMCs 1 and 4 (because they do not include the data of the main business applications).

Only AMCs 1, 5 and 6 carried out a regular test on their BCP during the period monitored. AMCs 2, 3 and 4 had an opportunity to test its robustness during the administrative lockdown period in the spring of 2020. It was noted, in this framework, that **all the AMCs of the sample group had implemented their BCP successfully during the lockdown period.** Note that this "full-scale" test enabled AMC 1 to observe the persisting need for paper processing in transactions such as the opening of securities accounts. An action plan was formally defined in response to this issue, including the **gradual introduction of the dematerialisation of transactions and digital signature** for the fund managers.

Regulatory reminder:

- AMCs shall establish and maintain effective business continuity plans aimed at ensuring, in the event of a disruption of their systems and procedures, the preservation of essential data and functions and the maintenance of their fund management activity, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their activities – Article 321-25 of the AMF GR (UCITS), Article 57 (3) of DR (EU) No. 231/2013 (AIFs), and Article 21 (3) of DR (EU) No. 2017/565 (investment firms).

Good practices:

- Setting out formally and updating an inventory of the IT equipment used, allowing tracking of the software versions used and identification of unallocated hardware.[49]
- Setting out formally a procedure for management of cyber incidents describing the process of reporting, feedback to management and data inputting to the compilation database.[50]

[49] Good practice already identified during the 2019 Cyber SPOT campaign.

[50] The summary of the 2019 Cyber SPOT inspection campaign pointed out a poor practice concerning a similar subject: "*Including cyber incidents in the operating incident management process, without a specific classification key (designed to facilitate the analysis and handling of underlying vulnerabilities)*".

- Setting up and keeping up-to-date a database of cyber incidents or, at least, identifying such incidents unambiguously when they are compiled in the database of operating incidents.
- Taking cyber risks into consideration in defining the business continuity strategy and ensuring regular testing of the firm's business continuity capabilities.
- Formally defining a plan for regular safeguarding of IT data, specifying the scope and frequency of the operations performed.
- Providing for the coverage of cyber risks in the insurance policies negotiated by AMCs for their business.

Poor practices

- Not formally defining the procedure for management of IS components and security patches.[51]
- Maintaining a password generation policy not complying with the ANSSI criteria.
- Allowing users to be administrators of their workstations.
- Retaining non-encrypted workstations (users or administrators).
- Not including in the BCP a continuity strategy in cases of (i) telephone outage or (ii) prolonged unavailability of the CIO.
- Not performing regular backup data restoration tests.

4.4- SUPERVISION OF PROCESSES FOR REMOTE ACCESS TO THE AMC'S IS

➢ *Processes for remote access to the AMC's IS by in-house personnel*

The personnel of all the AMCs of the sample group can remotely access their company's IS. The login process is available:

- either via personnel's **laptop computer**. This process is implemented by means of a Virtual Private Network ("VPN").[52] It gives full access to emails, shared network files and business applications;
- or via personnel's professional **mobile phone**. This process gives access **only to emails**, except for AMCs 4 and 6 for which access to the commercial contact management application is possible.

For all the AMCs of the sample group, the process of logging in by laptop computer via a VPN is secured by:

- Preventive controls:
  - authentication by a **specific**[53] combination of ID and password;
  - **filtering of VPN connections** by the firewall mentioned in section 4.3 above;
  - **encryption of data interchange via the VPN tunnel** opened between the employee's terminal and the company network;
- Detection controls: **automatic recording** of connections made by VPN to the enterprise IS.

[51] Conversely, the summary of the 2019 SPOT inspection campaign had highlighted the following good practice: “*Establishing IS administration procedures for all the equipment used (hardware and network).*”

[52] Refer to the glossary.

[53] This combination is different from that used by an in-house employee of the AMC to log in to a work session when they are in the office.

Since the data accessible remotely via employees’ mobile phones are restricted (as mentioned above), the arrangements for securing exchanges by this process are more limited for AMCs 1, 2, 3 and 5 and consist merely in authentication by a **specific** ID and password combination (different from that mentioned above). In addition, for AMCs 4 and 6, connections to access the commercial contact management application via mobile phone are **recorded automatically**. Lastly, as indicated in section 4.3 above, all the AMCs of the sample group have implemented in this area a **commercially available mobile terminal management tool**[54] which allows the remote deletion of data in cases of theft or loss (of the professional mobile phone, for example).

➢ ***<u>Processes for remote access to the AMC's IS by outside correspondents</u>***

Two types of outside correspondents are able to log in to part of the IS of the AMCs inspected.

Outside correspondents accessing the IS remotely	AMC 1	AMC 2	AMC 3	AMC 4	AMC 5	AMC 6
IT administrator	Yes	N/A[55]	Yes			N/A
Investors	Yes (access to an extranet)[56]	No[57]	No	Yes (access to the "dataroom" application)	Yes (access to an extranet)[58]	Yes (access to the "dataroom" application)

The system for remote access of **external IT administrators** to the IS of AMCs 1, 3, 4 and 5 is secured by using an encrypted **VPN** tunnel operating on the same model as that used for in-house personnel. Connections using this process are traced by AMCs 3, 4 and 5, **but not by AMC 1.**

The processes for remote access **by investors** to the IS of AMCs 1, 4, 5 and 6 concern two **areas**:

- The investors of AMCs 1 and 5 have access, via the AMC's website, to a dedicated extranet[59] portal containing the **regular reports on portfolio performance** and the necessary documents for knowledge of the customer. This remote access process is protected by the following **preventive controls**: access by password and encryption of the documents in the portal;
- The investors of AMCs 4 and 6 (specialised in private equity) have access to a "**dataroom**" application[60] allowing access to strategic and financial information concerning the companies in the portfolio. This remote access process is protected by **preventive controls** (access rules determined by the AMC according to the type of investor, with no link between the "dataroom" and the rest of the IS) and **detection controls** (periodic control of active access accounts, connection monitoring).

➢ ***<u>Processes for data interchange between the AMC and its partners</u>***

AMCs 1 to 5[61] have established data interchange flows between their IS and that of non-IT third-party service providers. The service providers in question are shown below.

[54] This type of tool is also called "*MDM*" for "Mobile Devices Management".

[55] AMCs 2 and 6 have insourced their IT administration function.

[56] Refer to the glossary.

[57] The fundholders and clients of AMC 2 have a link to the AMC's extranet which redirects them to the customer area of the depository/account-keeper website. However, these fundholders have no access to the AMC's IS.

[58] Refer to the glossary.

[59] This is a portion of the intranet for which access is extended to certain outside persons, in this case the clients of the AMCs in question. The external IT administrator of AMCs 1 and 5 does not have access to this extranet.

[60] AMCs 4 and 6 use the same "dataroom" application.

[61] Analysis of this aspect did not come within the scope of the conventional inspection of AMC 6 initiated at the end of 2019.

Service providers	AMC 1	AMC 2	AMC 3	AMC 4	AMC 5
Depository	x	x	x	x	x
Custody account-keeper	x	x			
Distributors					x
Fund auditor[62]	x	x	x	x	x
AMC auditor				x	x

AMCs 1 and 2 have formalised the electronic data interchange in place with the aforementioned service providers in the **sensitive data** mapping mentioned in section 4.1. This map specifies in particular the date of the last security check carried out by the AMC on the communication protocols used. However, **AMCs 3, 4 and 5 did not perform this work.**

No vulnerabilities were detected on these protocols during the inspections carried out, **except for AMCs 2 and 3**. The data interchanges (**in red** in the above table) carried out between **AMC 2 and its custody account-keeper** on the one hand, and between **AMC 3 and its auditor** on the other hand, are implemented via the File Transfer Protocol (FTP).[63] There is therefore a risk of unauthorised access to these data by a hacker becoming fraudulently positioned on the data flows between the AMC and its service provider.

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 - Article 321-24 of the AMF GR (UCITS), Article 57 (2) of DR (EU) No. 231/2013 (AIFs), and Article 21 (2) of DR (EU) No. 2017/565 (investment firms).

Good practices:

- Supervising the processes for remote access by employees to the AMC's IS by controls for both prevention (identification and specific connection password, encryption of the VPN tunnel) and detection (connection recording, MDM).
- Tracing remote access to the IS implemented by in-house or outside users via VPN.

Poor practice:

- Failing to take into consideration, in the sensitive data mapping, the data exchanges protocols in place with partners of the AMC (depository, account-keeper and statutory auditors in particular).

4.5- INTERNAL CONTROL OF THE CYBERSECURITY SYSTEM

➢ ***Permanent control of the cybersecurity system***

All the AMCs of the sample group included cyber risk control in their compliance and internal control plan ("PCCI"), **except AMC 6, even though its risk map mentions this.** This control is performed by the CICO for AMCs 1, 2 and 5 or by the delegated internal controller (for AMCs 3 and 4). However, this consideration of cyber risks in permanent control systems is **heterogeneous**. More specifically:

[62] Statutory auditor.

[63] The File Transfer Protocol is a protocol used on the internet for file swapping, generally used to download a file present on a server, or to send a file to a server.

- the **process of secure preservation of sensitive data** was subjected to formal controls, between 2017 and 2020, by AMCs 1 and 5, **but not by AMCs 2, 3 and 4** (even though this control is included in the compliance and internal control plan of AMCs 2 and 4);
- the process of coordination of outsourced IT services was subjected, between 2017 and 2020, to at least one formal control by AMCs 2, 3, 4 and 5, **but not by AMC 1.** For AMC 4, this control took the form of a review of a **security audit report conducted** on the administrator's IS;
- the process of cyber incident management was subjected, between 2017 and 2020, to at least one formal control by AMCs 1, 2, 4 and 5, **but not by AMC 3.**

➢ ***Periodic control of the cybersecurity system***

Unlike AMCs 1 and 2, AMCs 3, 4, 5 and 6 carried out security audits on their IT environment between 2017 and 2020. These audits took the following forms:

- For AMC 3, a security audit, carried out by an IS Security Audit Service Provider ("PASSI"), on the AMC's **website**. The work was completed by phishing tests;
- For AMC 4, a **network vulnerability test** on half of the AMC's physical facilities with a view to detecting paths of attack that could be taken by a potential hacker;
- For AMC 5, a **compliance check on the AMC's technical facilities in relation to its programme of operations** (performed in 2017 and 2020 by the delegated internal controller) and two technical test campaigns carried out by a "PASSI". The first campaign, in 2019, aimed at performing a pentest on the extranet. The second one, in October 2020, entailed performing a test to measure the **security level of the AMC's website** and the underlying servers;
- For AMC 6, a pentest delegated in July 2018 to a third-party service provider primarily targeting the level of security management **for the AMC's email service** (in line with the repeated attacks incurred during H1 2018 on the mailboxes of the entire line of command).

Regulatory reminders:

- ↗ If AMCs outsource the execution of operational tasks and functions that are critical or 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 GR (UCITS), Articles 318-58 to 318-61 of the AMF GR (AIFs), Article L. 533-10 II 4° of the Monetary and Financial Code and Articles 30 (1) and 31 of DR (EU) No. 2017/565 (investment firms).
- ↗ The AMC shall establish and maintain an effective compliance function that operates independently. This work notably involves controlling and regularly assessing the appropriateness and effectiveness of the policies, procedures and measures established and the actions taken to correct any failure by the AMC and the relevant persons to fulfil their professional obligations as mentioned 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 control function which is separate and independent from their other functions and activities and which has the following responsibilities: 1. 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. 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 GR (UCITS), Articles 61 (2) and 62 of DR (EU) No. 231/2013 (AIFs), and Articles 22 (2) and 24 of DR (EU) No. 2017/565 (investment firms).

Good practices:

- ↗ Having a pentest on the AMC's IS performed regularly by a specialized third-party service provider (preferably accredited by ANSSI), 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.[64]
- ↗ Asking key third-party service providers/partners to provide the reports on security audits that have been conducted on the portions of their IS or their departments interacting with the AMC's IS.

[64] Good practice already identified during the 2019 Cyber SPOT campaign.