EFAMA

European Fund and Asset Management Association

EFAMA RESPONSE TO THE COMMISSION'S CONSULTATION ON A POTENTIAL INITIATIVE ON THE DIGITAL OPERATIONAL RESILIENCE IN THE AREA OF FINANCIAL SERVICES

24 March 2020

Rue Montoyer 47 | B-1000 Bruxelles
T +32 2 513 39 69 | info@efama.org | www.efama.org
EU transparency register: 3373670692-24

EFAMA's response to the Commission's consultation on a potential initiative on the digital operational resilience in the area of financial services

Executive summary

As players in a globalised and technologically-driven financial services industry, asset management companies face cyber-security risks on a daily basis. Cyber-attacks aim mainly at obtaining, or restricting access to, sensitive data, related to clients and/or to portfolio construction and composition, trading and risk management, among other asset management functions. Recognising the global, pervasive and ever-changing nature of such threats, asset management companies have responded by adopting a variety of preventive measures to protect their clients, as well as their own business and reputation. These are modelled on existing and independent international standards for information security – particularly, the NIST, the COBIT and the ISO/IEC 27000 family standards - and are furthermore recognized and supported by the supervisory community of IOSCO as a whole. We believe it is therefore of paramount importance that such international standards be recognised *ex ante* and serve as a blueprint for the Commission's cross-cutting legislative review where relevant.

From this important preamble, our response develops EFAMA's views for each of the five main sections of the Commission's questionnaire, as follows:

- On **ICT and security requirements**, we reiterate the importance of existing cyber-security standards and caution the Commission against too rigid or prescriptive legislative solutions, which could ultimately also fragment global markets and harm the European asset management industry from a competitiveness standpoint;

- On **ICT and security incident reporting requirements**, EFAMA supports the development of a harmonised reporting template for individual companies to report incidents to their competent national cyber-security authorities. The latter should be the exclusive recipients of such information, in view of their technical expertise and confidential communication channels offered. With incidents being reported more consistently as a result, these specialised authorities should be encouraged in turn to present our broader industry with cyber-intelligence threat updates in view of improving prevention and detection;

- On **digital operational resilience testing frameworks**, we believe that sufficient resilience testing frameworks already exist in the form of requirements stemming from the aforementioned global standards. As a necessity, resilience testing in the form of "table-top" exercises must involve one or more (depending on core business location) competent national cyber-security authorities. The involvement of other public bodies should be strictly conditioned by their expertise and supervisory remit over asset management companies. In this regard, we strongly caution the Commission against entrusting the design and conduct of cyber-testing frameworks for our industry to pan-EU bank or macroprudential supervisors (i.e. ECB/SSM and ESRB);

- On **addressing third party risks and their oversight**, EFAMA is supportive of the Commission's approach to proceed through a general set of principles to orient financial market players when selecting third party service providers. Again, existing global standards (e.g. the ISO/IEC 27000 family) should serve as a model. In addition, we invite the Commission to consider a basic form of certification to be recommended for a category of third parties that the contracting company deems "critical" to its business. Typically these are providers with a dominant market position for their services, wielding unique technical expertise and significant pricing power. Experience has revealed

instances where such companies have refused to be audited by their contracting clients (including asset management companies), rendering an *ex ante* and ongoing assessment of their cyber-defenses difficult, where not impossible. Our considerations are also extended to potential business disruptions (e.g. in the form of sudden data cut-offs);

– Finally, on **other areas where EU action may be needed**, we favour the development of initiatives to foster more cyber-threat intelligence sharing among industry peers, as well as the gradual development of cyber-insurance policies.

Background: IOSCO Standards and cyber-risks from an asset management perspective

In April 2016, IOSCO published a final report entitled *Cyber Security in Securities Markets – An International Perspective*[1]. The report brought together the contribution of relevant IOSCO policy committees and related stakeholders to cover the main regulatory issues and challenges related to cyber-security for relevant segments of securities markets, including asset management companies.

As Affiliate Member of IOSCO and in cooperation with other regional trade associations representing investment managers within the standard-setter's Affiliate Members Consultative Committee (AMCC), EFAMA[2] has contributed to the final report's findings related to asset managers. Our inputs were drawn from the first IOSCO AMCC Cyber-Security Survey, administered annually to EFAMA's members (*inter alia*) since 2015 and aimed at assessing and reinforcing the cyber-security posture of the European asset management industry[3].

Based on our work performed under the *aegis* of IOSCO, the two key vulnerabilities to our industry are **data theft** (including client data/records, but also of portfolio holdings or anything market-sensitive by nature) and **data integrity** (including the manipulation of data - both proprietary or from third parties - employed across the firm, from portfolio construction, to technology-enabled advice ("robo-advice"), to trading). Consequently, an asset management company faces risks to its reputation, its ability to retain and grow its client base, along with other headline risks stemming from potential regulatory enforcement actions.

The findings from the past five iterations of the IOSCO AMCC Cyber-Security Survey confirm the following few, yet essential, good practices for preventive cyber-security:

– Identify the firm's key digital assets (including intellectual property, critical business processes, shareholder information and other confidential data, and key operating facilities) to allocate resources where the risks may be higher for the firm; firms should develop a clear understanding of normal network functions, activity, and links;

[1] Please access the Final Report (FR02/2016) on IOSCO's cyber-risk coordination efforts of April 2016 at the following hyperlink.

[2] EFAMA is the voice of the European investment management industry, representing twenty-eight member associations, fifty-nine corporate members and twenty-two associate members. At the end of the third quarter of 2019, the European asset management industry had total net assets of EUR 17.2 trillion, comprising almost 62,500 investment funds of which almost 34,000 were Undertakings for Collective Investments in Transferable Securities (UCITS) funds and almost 28,500 were European Alternative Investment Funds (AIFs).

[3] Since then, they survey is administered every year during the summer, on an anonymised basis, and jointly with other global buy-side trade associations, improving progressively in accuracy and in coverage. In 2019, a total of 113 non-US firms (from the original 80) participated across fifteen known jurisdictions (with twenty firms deliberately not indicating where they are based).

- Implement effective control and protection measures, involving, among other tools, adapted authentication mechanisms, control of administrative and privileged access, removal of "undesirable" applications, anti-virus protection, mobile device security, and encryption of data;

- Implement ongoing training for employees (including legal staff) and develop an effective security culture of responsibility and accountability throughout the firm;

- Ensure an appropriate monitoring of system and data usage to facilitate the identification of abnormal patterns;

- Develop detailed and actionable incident response plan, with clear roles and responsibilities, communication procedures and possible remediation measures; when an incident does occur, firms should be prepared to document their actions;

- Access and share actionable threat information, as well as building peer network to share expertise and increase circles of trust that include law enforcement;

- Engage with third parties to conduct due diligence reviews of a service providers' information security program, and understand if fourth party service providers are utilised; and

- Ensure an ongoing reassessment of the firm's cyber resilience, its vulnerabilities, and protection, including by benchmarking against industry practices and peers.

More recently, under the *aegis* of the International Investment Funds Association (IIFA), EFAMA has undertaken to publish an additional list of *Cyber-Security Program Basics* for smaller asset management companies, i.e. ones that potentially are less able to fully comply/implement existing international standards in light of resource constraints[4].

With this background, we now turn to provide our general views on the five main sections of the Commission's questionnaire.

1. ICT and security requirements

In light of their global cross-border operations, financial services companies – among which asset management ones – are vulnerable to cyber-threats. To prevent and tackle such threats in the interest of business continuity and for the well-being of their clients, asset management companies are already expected by their direct national supervisors to comply with at least one internationally recognised cyber-security standard. At present, relevant are the NIST[5], the COBIT[6] and the ISO/IEC 27000 family standards[7], recognised as cyber-security "core standards" by IOSCO in June 2019. Following an in-depth, cross-jurisdictional "gap analysis", IOSCO's conclusions expressly intended to avoid introducing new and potentially duplicative international standards[8]. Recognising that smaller companies may not have sufficient resources to conform fully with these more comprehensive standards, there are nevertheless

[4] Please refer to the IIFA *Cyber-Security Program Basics* published on 28 October 2019 and available at the following hyperlink.
[5] Please refer to the U.S. National Institute of Standards and Technology (NIST) cyber-security framework; available at the following hyperlink.
[6] Please refer to the Control Objectives for Information Technologies (COBIT) framework, administered by the global Information Systems Audit and Control Association (ISACA), available at the following hyperlink.
[7] Please to refer to the ISO/IEC 27000 family standards for IT, security techniques and information security management systems, developed by the International Standards Organisation (ISO) and International Electrotechnical Commission (IEC), available at the following hyperlink.
[8] In its Final Report to the IOSCO Board in June 2019, the organisation's Cyber Task Force has identified these as global "Core Standards". Please refer to the Final Report (FR09/2019) at the following hyperlink.

basic protocols already available to them[9]. The absence of references to these standards in the Commission's consultation document offers us reasons to be cautious around the outcome of the proposed cross-cutting legislative review. Moreover, we wish to recall that some European national supervisors have in turn also issued cyber-security guidance or codes for their domestic industry, in substance echoing the above standards.

We believe the proposed review should remain strictly targeted to address the existing *lacunae* in the relevant EU legislative texts, while minimising the introduction of additional requirements. Given the global nature of cyber-threats, the legislative review, we believe, should seek to build on and incorporate existing global standards, without necessarily proposing new ones *ex novo*. In conducting its targeted review, the Commission should in addition be mindful of avoiding uneven playing-field effects between global jurisdictions via stricter EU standards compared to the existing ones. For the European financial services industry, in which asset management companies play an integral part, such effects could bring about greater market fragmentation while also harming the global competitiveness of our industry *vis-à-vis* non-EU players.

In relation to a few specific questions from the Commission's questionnaire, we make the following remarks. Under Question 15, firms are asked whether legal clarity and simplification would be worthwhile in implementing security measures to manage ICT and security risks. In this regard, we note that meeting this end will require adherence to existing standards and codes of conduct, rather than "hard" legislation. As the Commission understands, only the former are malleable to be adapted as the cyber-threat environment evolves. Legal solutions thus risk being not adaptable and outdated quickly and will most likely be interpreted differently across borders (even within the EU). Similarly, Question 18 raises the prospect of legally defining the notions of "Recovery Time Objective" and "Recovery Point Objective" when several factors – often unknown – to a management company would make such objectives impossible to anticipate, let alone calculate. Also, we note that recovery times would also vary substantially depending on the type of business that is affected.

2. ICT and security incident reporting requirements

In principle, EFAMA supports the Commission's proposal to standardise ICT incident reporting across the various pieces of EU financial legislation. While we are not able to define a taxonomy of reportable incidents, nor advise on appropriate reporting templates in detail and timeframes, nor recommend specific materiality thresholds, we observe there is firstly a need to harmonise reporting templates for financial services companies to their respective cyber-security authorities. As templates presently vary considerably, including basic definitions of a "security incident", the quantity and quality of cyber-threat intelligence available to such authorities may be sub-optimal. A common template would therefore allow companies to report events more consistently between each other to the relevant cyber-security authorities. Moreover, such template should be consistent, where not merged, with the existing incident reporting requirements foreseen under the NIS Directive and GDPR regime, so as to avoid reporting overlaps.

In return for providing such authorities with timely information on one or more company-specific incidents, companies would greatly value, and reasonably expect, some feedback from the cyber-security authorities, in terms of alerts for common threats potentially affecting the same type of service providers, or even the broader market. Such two-way exchanges of cyber-threat intelligence are essential to enhance the degree of preparedness for our industry and national cyber-security authorities alike.

[9] For instance, apart from the IIFA's Cyber-Security Program Basics (above), smaller companies could model their cyber-defenses around the controls created by the Center for Internet Security (CIS Controls), comprising 20 basic, yet sufficiently comprehensive, controls. More information is available at the following hyperlink.

In terms of competence for receiving company-level reports on cyber-incidents, we believe this should reside exclusively with one or more (depending on a company's business presence) national cyber-security authorities designated by the NIS Directive, in light of their technical expertise and preparedness in receiving and processing sensitive information. In some jurisdictions, the cyber-security authorities may coincide with the direct industry supervisor. Where these authorities do not coincide with a company's direct supervisor, we recommend the latter receive relevant information only from the former (as is presently the case in most jurisdictions), so as to avoid overlapping reporting requirements for companies. Finally, the national cyber-security authorities should be prohibited from introducing any additional local requirements in terms of incident reporting.

3. Digital operational resilience testing framework

In line with our previous sections, we believe that resilience testing frameworks already exist in the form of specific global standard requirements companies already (or should) adhere to. Were the Commission, in line with the joint ESAs' advice, to consider developing an EU-wide cyber-resilience testing framework over the medium- to long-term, we believe that its design should necessarily build on such global standards. To be realistic, however, the testing framework should naturally include, apart from the asset management company, its key financial counterparts (e.g. depositary institutions, trading counterparties, exchanges, etc.) and one or more national cyber-security authorities (depending on the location of core businesses).

The involvement of pan-EU bodies, elicited under Question 31 of the Commission's questionnaire, should not be automatic, but decided case-by-case depending on these bodies' regulatory remit and experience with the asset management industry. We would consider the involvement of ENISA as a possibility, in light of its expertise and coordinating role among national cyber-security authorities. Entrusting other pan-EU bodies, especially those responsible for banks and macroprudential topics like the ECB/SSM and the ESRB would be counterproductive. This would lead to biased testing frameworks – precisely because designed around credit institutions - being imposed on non-bank actors like asset managers. Among these frameworks, we cite the cyber-resilience testing guidelines designed for credit institutions as those published in November 2019 by the EBA (EBA/REC/2017/03), as well as the earlier March 2018 recommendations on outsourcing to cloud service providers (EBA/GL/2019/04). Such standards would in our view be inappropriate if applied to the asset management industry, in light of the substantially different nature of its business, and potentially also conflict with sectoral requirements stemming from the UCITS, AIFMD and MiFID II frameworks. In this regard, testing frameworks should embed the principle of proportionality, thereby calibrating ICT and security risks in light of the nature of a company's activities and services, as well as on the scale and complexity of its operations.

We do recognise that for asset management companies that are subsidiaries of larger bank or insurance groups, cyber-security testing, along with other cyber-security practices, are typically performed at a consolidated group parent level. In such instances, important is that asset management subsidiaries should not apply the parent's standards by default, but those requirements stemming from their own sectoral legislation and to the extent these do not conflict with those of the parent undertaking.

In relation to Questions 30 and 31 of the questionnaire, we advise the Commission to be particularly cautious if attempting to draw a "one-size-fit-all" distinction between what is a "baseline" case versus one that would require a "more advanced" type of test (e.g. TLPT). Each asset management company – as other actors in the financial services industry – is solely capable to determine the materiality of a threat on the basis of its unique business. We thus do not believe that future "significance" assessments by the Commission – as per Question 31 of the questionnaire – are possible, as only the firm itself can determine which of its operations requires more advanced testing on the basis of the existing global standards. Consequently, we strongly object to such tests being made compulsory, as referenced in the same question.

4. Addressing third party risk: Oversight of third party providers (incl. outsourcing)

EFAMA welcomes the Commission's approach to proceed through a set of general principles embedded in a future EU framework as a guide to orient and protect financial market players when selecting third party service providers and drafting the related agreement terms. Asset management companies – as other financial market players - make ample use of third parties (e.g. fund administrators, depositary banks, distributors, data vendors, etc.) for their operations, although these should not be confined to the financial sphere. Experience has proven that financial firms have suffered attacks from less-likely sources, albeit with permission to access the firm's network (e.g. advisory services, logistics, catering, office climatisation, etc.).

Sound principles in this regard for creating an "extended trust" environment between the contracting firm and contractor are multiple, ranging from a fair and transparent tender-based onboarding to the specification of IT security requirements and identification of sensitive information; from the related management procedures (including controls to identify unique risks) to the contracting firm's right to audit the contractor where possible (including its own cyber-defenses), identifying possible non-compliance cases and ensuing penalties *ex ante*, etc. Naturally, the contracting firm's due diligence – initial and throughout the lifecycle of the service agreement – should also consider vulnerabilities from fourth or fifth party service providers more remotely. Finally, the terms of the service agreement should address vulnerabilities arising at the end of a business relationship (e.g. non-compete clauses). We recommend the Commission refer to the extensive ISO/IEC 27000 family of standards in this respect.

There may be instances where, given the particular set-up of a company's supply chain, a basic form of certification for certain "critical" third party service providers to adhere to could prove beneficial. The main justification behind this idea lies in the often encountered refusal by key third party providers to be audited by their prospective contracting clients, reinforced by the fact that the former also concentrate market power as *de facto* oligopolists or monopolists (e.g. large cloud service providers) in one specific service domain. By certifying a third party's adherence to a comprehensive and internationally accepted cyber-security standard, this would foremost facilitate the onboarding of such critical third parties for the contracting company, thereby avoiding the protracted negotiation of service contracts to ensure that third parties can abide by essential best practices. In other terms, such certification would remove the need for contracting companies to have to conduct in-depth audits of a third party contractor, an operation made particularly strenuous if the contractor is a near monopolist, has unique technical IT expertise, or wields a significant pricing power for its services. Through certification, asset management companies as contracting parties – especially medium-sized, or smaller ones with less negotiating power – could furthermore draw sufficient comfort and justify their choice of one third party service provider over another *vis-à-vis* their own direct supervisors in the event of an examination. Although we do not believe such certification should be mandatory, it should at least be recommended for those third party contractors deemed "critical" to the operations of the contracting parties.

Assessing whether a third party contractor is "critical" to an asset management company is a decision that should reside solely with the latter. Quantitative and qualitative information will be essential, as will the other considerations listed under Question 37 of the Commission's questionnaire. Yet, these elements must reflect the company's unique operational model, its unique client base and product/service mix, its end-to-end supply chains, along with other defining aspects which cannot be aggregated for the sole purpose of producing an EU-wide oversight ICT framework. These sensitive appreciations will inevitably be missed in any over-arching framework, leading us to conclude that a "bottom-up" approach remains the best solution, whereby asset management companies would help design a more "tailored" oversight framework to include critical third party service providers, together with their cyber-security authorities and main market supervisors of reference.

In relation to Question 38 of the questionnaire, we do not believe that the heavy-handed regulatory approach to mandate the rotation of third party ICT providers would be beneficial. Asset management companies place a great premium on building long-founded and trustworthy business relationships with key third party ICT providers, which have an equal interest in managing cyber-security risk as their own. Continuous engagement with, and investments by, third party ICT providers to counter emerging cyber-risks would in our view be a far more practical solution as opposed to mandating the periodical rotation between providers, the imposition of a multi-provider approach, or artificial regulatory limits to cap reliance on one specific third party provider. Moreover, at the present state and for the foreseeable future, the offer of such services (e.g. cloud technology and data feeds) is and will remain concentrated in the hands of a very few (less than a handful of) global firms. It is certain that any mandatory regulatory change will in this respect be highly disruptive and work against the interests of all investors.

Yet, there are aspects of asset managers' relationship with critical third party providers that would benefit from explicit regulatory provisions. These relate, in particular, to the potential early termination of data contracts as a result of a cyber-incident affecting the third party. As the Commission understands, asset management companies make an extensive use of data streams in their daily operations (e.g. from the design of a client's portfolio, to trading its components and managing its risks). These services are bought at a significant cost from a restricted group third party data providers and vendors, which together constitute an oligopoly, where not a monopoly in some instances. Our industry is at risk of experiencing severe data cut-offs dealt by these actors were these to be impacted by a cyber-incident threatening the integrity of their data, or more broadly, in the event of contractual disputes. This would certainly lead to a substantial impairment of an asset management company's core operations and consequent economic harm to its clients. As presently such third party data providers and vendors are regulated in the EU only by general company law provisions, we believe that these actors should be obliged to (i) declare their conformity to one or more of the global cyber-security standards mentioned above, (ii) conduct extensive cyber-threat penetration testing of their systems to ensure data integrity, and (iii) avoid sudden cut-offs in relation to the critical data feeds they provide to a wide host of financial market players including asset management companies.

5. Other areas where EU action may be needed

Information sharing

EFAMA fully supports any initiative aimed at fostering greater cyber-threat intelligence sharing of financial market entities among their industry peers.

Promotion of cyber-insurance and other risk transfer schemes

The market of insuring against cyber-risks remains presently underdeveloped across Europe, although stands to benefit from a considerable demand, as awareness around cyber-threats grows and estimations of potential resulting damages/losses from data breaches and business interruptions become more accurate.

For smaller firms with more limited capabilities, a cyber-insurance policy often also promises access to best-in-class cyber-security programme administered through the insurer or via a recommended third party, including access to additional skills the former may not have in-house, such as access to cyber-forensic investigators, legal teams and communications professionals.

xxx