AUTORITÉ DES MARCHÉS FINANCIERS

16 December 2019

The AMF publishes a review of its thematic inspections of the cybersecurity systems in place in asset management companies

In accordance with its supervision priorities for the current year, the Autorité des Marchés Financiers reviewed the cybersecurity systems of five asset management companies. Based on its observations, it highlights the good practices noted.

During these short thematic inspections called "SPOT" (Supervision des Pratiques Opérationnelle et Thématique - operational and thematic supervision of practices), the regulator examined:

- the organisation of cybersecurity systems with regard to human and technical resources;
- the governance of these systems;
- the Information System administration and surveillance systems; the cyber incident management process;
- the management of sensitive data;
- the business continuity plan;
- existing internal control of the Information System and the cybersecurity system.

For performing its work, the AMF considered cyber risk as arising from any potential malicious attack, internal or external, on one of the key features of the Information System of an asset management company (AMC), namely its availability, its integrity, the confidentiality of the data that it processes or the traceability of the actions performed in the Information system.

In this context, the AMF noted that the firms inspected are starting to address cyber risk by including it in their risk mapping, by compiling the cybersecurity incidents that they sustain and by calling on specialised service providers to verify the robustness of their Information System from time to time. However, the systems analysed do not take into account the potential impacts of the materialisation of cybersecurity risks on the firms' regulatory compliance with regard to (i) ensuring the level of regulatory capital, (ii) retention of sensitive data, (iii) maintenance of an effective business continuity plan, and (iv) maintenance of appropriate (IT) resources.

The AMF also noted the practically universal absence of mapping of (i) sensitive data and (ii) critical systems, and of a data classification policy, leading to a risk of partial coverage of major risks by the control system. Moreover, the formal identification of cyber incidents for continuous assessment of the associated risk level proves problematic in the existing compilation databases. Lastly, the vulnerabilities identified or confirmed by internal control are not corrected with sufficient speed and monitoring.

For asset management companies belonging to a Group (most of the tested sample), inadequate internal supervision of the services (relating to IT, cybersecurity and business continuity) performed by the parent company was identified. But the technical execution of these services by the Group cannot exempt asset management companies from their responsibilities regarding the definition (in priority) of the main risk areas and management of the relevant controls.

Among the best practices observed, the AMF notes, for example, the following:

- Ensuring the independence of the CISO (Chief Information Security Officer) function relative to the IS Department (Information Systems Department) either by (administrative or functional) reporting by the CISO to the Executive Committee, or by establishing a control function independent of the CISO's activities;
- Raising the AMC's employees' awareness of cybersecurity risks by including them in the annual training plan and, at least once a year, performing a test on employees' reaction to attempted phishing by email;

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

Conversely, the AMF noted the following poor practices:

- Deploying a cybersecurity system in the absence of (i) prior identification, (ii) classification by criticality level (on the basis of the AICT criteria) and (iii) regular review of sensitive data and Information Systems;
- In AMC risk mapping, confining the analysis of cybersecurity risks solely to the impacts of operational risk on the funds and/or portfolios managed;
- Not blocking the USB ports of user workstations;
- Deploying the process of permanent/periodic control of sensitive outside IT service providers on the basis of a non-exhaustive list of said providers.

Apart from the summary published on this day, this series of SPOT inspections gave rise to the sending of follow-up letters to the AMCs in question. Cybersecurity risks will be the subject of other AMF inspections in the coming months. In light of the observations made on completion of these inspections, the AMF plans to work out a specific cybersecurity policy proportional to the size of the players.

About the AMF
The AMF is an independent public authority responsible for ensuring that savings invested in financial products are protected and that investors are provided with adequate information. The AMF also supervises the orderly operations of markets. Visit our website https://www.amf-france.org

Read more

↘ Summary of SPOT inspections on cybersecurity systems of asset management companies

ON THE SAME TOPIC

Subscribe to our alerts and RSS feeds

AMF NEWS RELEASE

SUPERVISION

26 November 2020

Asset management: the AMF finds the effectiveness of internal control outsourcing processes to be too disparate

AMF NEWS RELEASE

SUPERVISION

29 September 2020

The AMF publishes the findings of its SPOT inspections on the valuation of complex financial instruments

NEWS

SUPERVISION

21 July 2020

The AMF publishes the summary of its SPOT inspections on Record-keeping

Legal information:
Head of publications: The Executive Director of AMF Communication Directorate. Contact: Communication Directorate – Autorité des marches financiers 17 place de la Bourse – 75082 Paris cedex 02