ESAs publish Joint Advice on Information and Communication Technology risk management and cybersecurity

Regarding **the need for legislative improvements,** in developing the Joint Advice the ESAs' objective was that every relevant entity should be subject to clear general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. Guided by this objective, the proposals presented in the Advice aim at promoting stronger operational resilience and harmonisation in the EU financial sector by applying changes to their respective sectoral legislation. Incident reporting is highly relevant to ICT risk management and allows relevant entities and authorities to log, monitor, analyse and respond to ICT operational, ICT security and fraud incidents. Therefore, the ESAs call for streamlining aspects of the incident reporting frameworks across the financial sector. Furthermore, the ESAs suggest that a legislative solution for an appropriate oversight framework to monitor the activities of critical third party service providers should be considered.

Regarding the **costs and benefits of a coherent cyber resilience testing framework**, the ESAs see clear benefits of such a framework. However, at present there are significant differences across and within financial sectors as regards the maturity level of cybersecurity. In the short-term, the ESAs advise to focus on achieving a minimum level of cyber-resilience across the sectors, proportionate to the needs and characteristics of the relevant entities. Furthermore, the ESAs propose to establish on a voluntary basis an EU wide coherent testing framework together with other relevant authorities taking into account existing initiatives, and with a focus on Threat Lead Penetration Testing (TLPT). In the long-term, the ESAs aim to ensure a sufficient cyber maturity level of identified cross-sector entities.

To implement the proposed actions, the ESAs highlight the required legal basis and explicit mandate, which is necessary for the development and implementation of a coherent resilience testing framework across all financial sectors by the ESAs in cooperation with other relevant authorities.

Background

The European Commission's March 2018 FinTech Action Plan specifically requests the ESAs:

- To map, by Q1 2019, the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate a) to consider issuing guidelines aimed at supervisory convergence and enforcement of ICT risk management and mitigation requirements in the EU financial sector and, b) if necessary, provide

the Commission with technical advice on the need for legislative improvements.

- To evaluate, by Q4 2018 (now Q1 2019), the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.