EBA publishes guidelines on ICT and security risk management

28 November 2019

**The European Banking Authority (EBA) published today its final Guidelines on ICT and security risk management. These Guidelines establish requirements for credit institutions, investment firms and payment service providers (PSPs) on the mitigation and management of their information and communication technology (ICT) and security risks and aim to ensure a consistent and robust approach across the Single market. These Guidelines will enter into force on 30 June 2020.**

The increasing digitalisation in the financial sector and the growing interconnectedness across financial institutions and third parties make financial institutions’ operations vulnerable to internal and external ICT and security risks that can potentially compromise their viability. As a result, sound ICT and security risk management are key for a financial institution to achieve its strategic, corporate, operational and reputational objectives.

These Guidelines set out expectations on how all financial institutions should manage internal and external ICT and security risks that they are exposed to. This guidance also provide the financial institutions with a better understanding of supervisory expectations for the management of the said risks, covering sound internal governance, information security requirements, ICT operations, project and change management and business continuity management.

The Guidelines also cover the management of PSPs’ relationship with payment service users (PSUs) to ensure that users are made aware of the security risks linked to the payment services, and are provided with the tools to disable specific payment functionalities and monitor payment transactions.

The Guidelines are addressed to credit institutions and investment firms as defined in the Capital Requirements Directive (CRD), for all of their activities, and to PSPs subject to the revised Payment Services Directive (PSD2), for their payment services.

**Legal basis and next steps**

These Guidelines build on the provisions of Article 74 of Directive 2013/36/EU (CRD) that mandate the EBA to further harmonise financial institutions' governance arrangements, processes and mechanisms across the EU regarding internal governance, and derive from the mandate to issue guidelines in Article 95(3) of Directive (EU) 2015/2366 (PSD2) with regard to the establishment, implementation and monitoring of security measures for operational and security risks.

These Guidelines respond to the European Commission's FinTech Action plan request for the EBA to develop guidelines on ICT risk management and mitigation requirements in the EU financial sector.

The EBA Guidelines will enter into force on 30 June 2020. The Guidelines on security measures for operational and security risks under PSD2 (EBA GL/2017/17) issued in 2017 have been fully integrated into these Guidelines and will be repealed once these Guidelines become applicable.