

3 April 2020

## **EBF KEY MESSAGES ON THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON A DIGITAL OPERATIONAL RESILIENCE FRAMEWORK FOR FINANCIAL SERVICES: MAKING THE EU FINANCIAL SECTOR MORE RESILIENT AND SECURE**

- The EBF welcomes the initiative of the European Commission to bring forward legislative proposals for fostering the digital operational resilience framework for financial services with a view to harmonise rules across the EU. The interconnectedness of all actors within the financial ecosystem, incl. third party providers, and the evolution of ICT risks highlight the need for a **common level of minimum security for the financial sector as a whole**, based on international coordination.
- Financial institutions already abide by different existing security frameworks that establish measures for ensuring the resilience of the banking system (e.g. NIS Directive, PSD2, MiFID II, CRD2, e-IDAS, GDPR, EBA Guidelines on ICT and security risk management, BIS CPMI-IOSCO Guidance on Cyber resilience for financial market infrastructures, TIBER-EU, EBA Guidelines on outsourcing, ECB IT risk self-assessment questionnaire). Any new requirements should be **harmonised** and also **aligned with existing rules at EU and global level**, to avoid duplications or overlaps.
- New rules should follow a **risk-based** approach. This would ensure that the framework is **future-proof** and will provide entities the flexibility required to adapt based on the continuously evolving nature of cyber and technology risks.
- It is important for financial institutions to **report once**; multiple different legal requirements at EU and national levels currently impose significant regulatory and operational burdens on banks. Effective incident reporting should be **simplified, clarified on its purpose** and combined with **feedback from the supervisors**. Reporting thresholds should be pragmatic and focus on significant security incidents, e.g. having impact on operational effectiveness of core banking functions. Fundamental for an effective incident reporting framework is the use of a common language and a **standardised taxonomy**, based on internationally agreed rules.
- Rules regarding the implementation of **oversight of third party providers**, which would **preferably be at European level on the basis of international coordination**, should be risk-based according to the type/ criticality of the service and they should target these providers without imposing additional requirements for banks.

## About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The EBF is committed to a thriving European economy that is underpinned by a stable, secure and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

[www.ebf.eu](http://www.ebf.eu) @EBFeu

### For more information:

#### **Alexandra MANIATI**

Director  
Cybersecurity & Innovation  
[a.maniati@ebf.eu](mailto:a.maniati@ebf.eu)

#### **Iliana KOUTOULAKOU**

Policy Adviser  
Compliance, Tax & Security  
[i.koutoulakou@ebf.eu](mailto:i.koutoulakou@ebf.eu)