EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

COMMENTS ON THE DRAFT "CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES"

Name of the originator (i.e. name of the company or association)	German Banking Industry Committee (GBIC)	ISO code of the country of the originator	DE

Comments on the draft Cyber Resilience Oversight Expectations for Financial Market Infrastructures

Issue	Comment	Reasoning
General	Clarification	It is undisputed that the topic of "cyber resilience" is of great importance. Nevertheless, IT security requirements should be aligned with the systemic relevance and criticality of the infrastructure, on the one hand, and the need for protection on the other hand, and should be formulated proportionally depending on this. The ECB's Consultation Paper sets out expectations for cyber resilience for financial market infrastructures without defining them unambiguously. We therefore consider it necessary to define the concept of Financial Market Infrastructure to clarify who/what the ECB addresses exactly. It is important for institutions to recognize whether, and if so to what extent, they are affected by ECB expectations. Here, the remarks in the Committee on Payments and Market Infrastructures paper "Guidance on cyber resilience for financial market infrastructures" of June 2016 (CPMI-IOSCO Guidance on FMEs) should be reflected - also see page 7 of the ECB consultation paper on Background of the formulated expectations. According to 1.3.1 of the CPMI-IOSCO Guidance on FMEs, the target group is defined as follows: "This guidance is first and foremost directed to FMIs as defined in the PFMI, namely: systemically important payment systems, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs)."

General	Clarification	Although the relevant supervisory authorities under the CPMI-IOSCO paper on FMEs may decide to extend this guidance to other types of infrastructures that are not formally covered by the CPMI-IOSCO Guidance on FMEs, at least for payment systems, the specific ECB requirements should only to be considered if these infrastructures are systemically important or critical. What should be classified as critical should be assessed according to the national IT security laws or national regulations issued thereon. In Germany, for example, this is the BSI-Kritis-Verordnung, which determines critical infrastructures. These regulations implement the requirements of the Directive on security of network and information systems (NIS Directive) (EU) 2016/1148 on measures to ensure a high common level of security of network and information systems in the European Union. For all other systems, there are sufficient supervisory requirements, formulated in proportion and based on the protection needs of the systems. In Germany e.g. these are the "Banking Supervision Requirements for IT" published in November 2017 ("BAIT"), which have to be observed by the banks and which specify the minimum requirements for risk management (MaRisk). The MaRisk itself was again adjusted in October 2017 with regard to the IT requirements and the focus on the protection requirements of the systems. In addition, the guidelines on internet payments security of the EBA are to be observed, in Germany by the minimum requirements for the security of Internet payments (MaSI) are implemented. Further payment protection requirements, in particular for strong customer authentication, will be implemented as part of the implementation of Payment Service Directive 2 and Delegated Regulation (EU) 2018/389. In this respect, there are no additional requirements for non-systemically relevant and non-critical infrastructures necessary. Against this background, we ask that the scope of the paper be concretized in order to ensure a proportional application in which the costs, risks and benefits are proportionate.

General	Amendment	We support the overall set of expectations for FMIs as well as the ECB's decision to provide their views in the form as guidance, rather than prescriptive rules, to allow for the needed flexibility for FMIs to adapt to the evolving cyber landscape. As part of this process, FMI are expected to assess their own capabilities and engage with external stakeholders to enhance the cyber-resilience of its overall ecosystem. This may include consideration around testing, contingency planning, resumption and recovery planning, amongst other things. Given the broad range of entry points through which an FMI may become compromised, and the interconnected nature of the FMI network, external engagement with FMI participants is indeed prudent. However, consideration should be given to the extent to which constant and disparate engagement from individual FMIs may impact a financial institution's own efforts to enhance cyber-resilience. This engagement may be particularly concerning if FMIs follow heterogeneous approaches (e.g. specific/non-harmonized control frameworks, self-attestations, questionnaires, joint exercises, certifications, etc.), imposing unnecessary burdens on FMI stakeholders which would have the effect of diverting valuable resources away from managing own cybersecurity programs.