EBA CLEARING

EBA CLEARING comments on the consultative report on cyber resilience by the Committee on Payments and Market Infrastructures (CPMI) and the Technical Committee of the International Organisation of Securities Commissions (IOSCO)

23 February 2016

About EBA CLEARING

EBA CLEARING is a bank-owned provider of pan-European payment infrastructure solutions. The Company was established in June 1998 by 52 major European and international banks with the mission to own and operate EURO1, the only privately owned RTGS-equivalent large-value payment system on a multilateral net basis. Since 2000, EBA CLEARING has been running the STEP1 single payment service on the EURO1 platform, which is geared at medium-sized and smaller banks. EBA CLEARING also owns and operates STEP2-T, a Pan-European Automated Clearing House (PE-ACH) for processing euro retail payments. Today, EBA CLEARING counts over fifty shareholder banks and, through its EURO1 and STEP2-T systems, offers both high-value and low-value clearing and settlement services to a wide community of banks in the European Union.

Both EURO1 and STEP2-T have been classified by the Eurosystem as systemically important payment systems. The systems are held to the highest oversight requirements as laid down the in Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB 2014/28), which implements and is consistent with the "Principles for financial market infrastructures" (PFMIs), introduced in April 2012 by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements and the International Organization of Securities Commissions (IOSCO). The European Central Bank is the Competent Authority for the oversight of the EURO1 and STEP2-T systems.

EBA CLEARING welcomes the opportunity provided by the CPMI and IOSCO to comment on the consultative report on cyber resilience.

General comments

CPMI and IOSCO have issued a report with guidance, which, thanks to its resemblance to the "Framework for Improving Critical Infrastructure Cybersecurity", issued by the National Institute of Standards and Technology (NIST) in February 2014, could provide a structure to an FMI to manage its cyber risk.

Although CPMI and IOSCO claim that their guidance is not meant to introduce new or additional requirements as compared to the PFMI, section 2 on 'governance' and section 9 on 'learning and evolving' provide guidance which is not easily linked to Principles and Key Considerations from the PFMI report, and in practice do constitute new requirements. Whereas in section 9 mostly new requirements are introduced, the section on governance contains elements which go beyond what is in the PFMI (e.g. the requirement to have a separately documented cyber resilience framework next to the comprehensive framework for the management of risks).

Another general comment is related to the fact that the consultative paper does not include a 'cyber resilience assessment methodology', nor an indication of how to link the guidance to the existing CPMI-IOSCO assessment methodology and rating. This omission will give rise to different interpretations by authorities when assessing an FMI and may create an uneven playing field. It is of the utmost importance that authorities apply the requirements and assess compliance in a uniform manner.

An example where clear assessment criteria are lacking is section 9 on 'learning and evolving', where somewhat vague requirements are introduced such as: an FMI should aim to instil a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

Also, the consultative report lacks a timeline indicating by when FMIs are expected to comply with the guidance. Such a timeline is relevant in two ways: (1) some guidance constitutes a new requirement. Those requirements which have an impact on the Companies governance as SIPS operator would attract an implementation program of up to 2 annual governance cycle, and those requirements that would have an impact on e.g. elements of the design of our payment systems would attract a period of up to 2 years for implementation; (2) some guidance requires an FMI to cooperate and coordinate with its eco-system and thus the FMI is dependent on others and this typically requires a significant lead time before actual accomplishments can be obtained. Therefor a transition period of two years to comply with the eventual guidance would seem opportune.

An aspect not covered in the Guidance report is whether CPMI and IOSCO intend to extend the guidance on cyber resilience for FMIs to critical service providers (CSP) (currently covered by Annex F), and whether CSP's are expected to demonstrate that they meet the requirements from the cyber guidance as well. If so, the question is also whether FMIs can continue to rely on oversight arrangements for CSPs by national authorities (alone or in cooperation) which are already in place. The alternative would be that FMIs individually need to assess a CSP's cyber resilience, which in the opinion of EBA CLEARING is not efficient and should be avoided.

The guidance under consideration fails to strike a balance between - or even mention - cyber resilience and Principle 21 which requires an FMI to be efficient in the sense that it should also consider the practicality and costs of a system for participants, their customers, and other relevant parties (including other FMIs). If not applied consistently to all types and sizes of FMIs, extensive cyber risk requirements drive up the costs for systemically important FMIs, which have to be borne ultimately also by participants. As a consequence, participants may choose an alternative arrangement which is less costly but may pose increased risks to the financial system and the broader economy due to its lower level of resilience.

To conclude the general comments, one important comment relates not particularly to the guidance on cyber resilience as such, but concerns Principle 23 on Disclosure. CPMI and IOSCO require FMIs to publically disclose relevant rules and key procedures, and to disclose clear descriptions of a system's design and operations to its participants. This requirement from the PFMI could be at odds with an effective protection against cyber-attacks; cyber resilience is best achieved by safeguarding information on system design, etc. Disclosure of information as required by Principle 23 provides valuable insights to attackers. EBA CLEARING would appreciate particular attention by CPMI and IOSCO to this comment in the final guidance report.

Comments on the content

In section 2, the CPMI and IOSCO define the concept of cyber governance as the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. Fundamentals and elements of cyber governance are a cyber resilience strategy, a cyber resilience framework, defined objectives, assigned roles and responsibilities, communication with stakeholders, etc. Some of these elements should of course be taken up by an FMI. However, the guidance from CPMI and IOSCO would benefit from a clarification and arguments on why an FMI should have a cyber resilience framework which is different from its comprehensive risk management framework and why 'cyber risk' should be governed differently from other risks. More fundamental is the fact that new requirements labelled as guidance at the same time create an unbalance in the requirements being applied to FMIs. Where the PFMI were supposed to set a common base level of risk management across FMIs, and thus the requirement for an FMI to take an integrated and comprehensive view of its risks, the current guidance does not sufficiently reflect that cyber is an aspect of operational risk, which is one of several risk categories FMIs are confronted with. EBA CLEARING clearly favours one comprehensive risk management framework instead of multiple topical frameworks. This is not only more efficient, EBA CLEARING is of the opinion that integration is ultimately also more effective.
In its current form, some of the guidance appears to bring additional bureaucracy to an FMI[1] and in some cases CPMI and IOSCO seem to have moved away from principle based guidance. E.g. the requirement to designate a senior executive to be responsible and accountable overall for the cyber resilience framework within the organisation, which is linked to the observation that FMIs have grown reliant on ICT systems, suggests that such an executive should come from within the IT department and thus leaves little freedom for an FMI to organise itself at senior management level.

The consultative document aims to provide guidance for FMIs to enhance their cyber resilience. However, in some cases the guidance remains unnecessarily unclear (vague) and CPMI and IOSCO are asked to clarify. An example is section 9.3.1: 'Metrics and maturity models allow an FMI to assess its cyber resilience maturity against a set of predefined criteria, typically its operational reliability objectives. This benchmarking requires an FMI to analyse and correlate findings from audits, management reviews, incidents, near misses, tests and exercises as well as external and internal intelligence gathered. The use of metrics can help an FMI to identify gaps in its cyber resilience framework for remediation, and allow an FMI to systematically evolve and achieve more mature states of cyber resilience.' The guidance on metrics as is, is a general statement and CPMI and IOSCO do not provide any practical example of which metric(s) - either from theory or actual examples from anonymised FMIs - could be used by FMIs and thus the 'guidance' does not guide FMIs towards enhancing cyber resilience.

The consultative report stresses the existence of interconnections and importance of approaching recovery with participants, interdependent FMIs, authorities and service providers and the FMIs appear to be given the most active role in this respect. The report however remains vague with regard the role authorities could or will play and CPMI and IOSCO are asked to provide more clarity, in particular with respect to reaching out

[1] This primarily is the case for the requirement to devleop a cyber resilience framework "which should be consistent with the enterprise operational risk framework", but also applies to section 3.2.1. A similar exercise to identifycritical business functions and processes had to be conducted in the context of recovery and orderly wind down planning.

themselves to stakeholders such as credit institutions, service providers and technology companies. Similarly, the role of authorities with regard to testing (section 7.2.1), enabling access to cyber threat intelligence in the context of geopolitical developments (which is often labelled confidential or secret and thus not easily accessible and readily available to FMIs) (section 8.2), and so-called multilateral information-sharing arrangements (section 8.3.2) should also be made more explicit.

In section 6.3.1 CPMI and IOSCO refer to the requirement to resume operations within two hours of a disruption caused by a cyber incident, the two hours stemming from 'traditional incidents' affecting availability rather than integrity. EBA CLEARING is of the opinion that a controlled resumption of operations in extreme but plausible scenario's, such as those evolving around software integrity, data integrity or the loss of data as such, should not be hampered by decision making and actions under time pressure. EBA CLEARING is of the opinion that restoration of integrity within two hours is aspirational and that the restoration of integrity prevails over a (too) hasty resumption for the sake of speed alone. A cyber-attack just cannot be compared to traditional incidents which impact the availability of systems.
In this context, EBA CLEARING would also appreciate further guidance and clarification on section 6.4.5 'forensic readiness'. Resumption in two hours is difficult to reconcile with the forensic investigative process to safeguard logs and evidence, which is likely to take more than two hours, especially since the safeguarding of such evidence could be subject to strict protocols for the evidence to be admissible in a judicial process.

Also in relation to the two hour RTO, CPMI and IOSCO state that the possibility of a so-called non-similar facility (NSF) solution to resume operations after a cyber-attack as one of the options may be taken into account. EBA CLEARING appreciates that a NSF is not a requirements per se. Given the likely costs for the development and especially maintenance of a NSF and other downsides, EBA CLEARING favours investing in alternative processes rather than in systems.

As a minor comment, the guidance on 'IT security hygiene', i.e. the basic IT and IT security controls any organisation should have in place, e.g. listed in section 4.2.3 and 4.4.3 - and although essential to an effective cyber risk management - does not provide new insights and could be removed from the report.

To conclude our reply to the public consultation, should you wish any elaboration on the comments made, EBA CLEARING is more than willing to respond to such request.