EUROPEAN CENTRAL BANK
EUROSYSTEM

Response to the public consultation on the cyber resilience oversight expectations

Cyber resilience oversight expectations: outcome of the public consultation

1 Introduction

In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the Guidance on cyber resilience for financial market infrastructures (Guidance)[1], which requires financial market infrastructures (FMIs) to immediately take the necessary steps to implement it, together with relevant stakeholders, to ensure that they enhance their levels of cyber resilience. The Guidance has been developed to further supplement the Principles for financial market infrastructures (PFMIs)[2], which the Committee on Payment and Settlement Systems (CPSS) and IOSCO published in April 2012, and the ECB's Governing Council adopted on 3 June 2013 for the conduct of Eurosystem oversight in relation to all types of FMIs.

In this context, the ECB launched a public consultation on the draft cyber resilience oversight expectations (CROE) from April to June 2018. The CROE serves three key purposes. It provides: (i) FMIs with detailed steps on how to operationalise the Guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; (ii) overseers with clear expectations to assess the FMIs for which they are responsible; and (iii) the basis for a meaningful discussion between the FMIs and their respective overseers.

The ECB received responses from 20 entities, including FMIs, banks, banking communities and associations. The ECB wishes to thank all respondents for their valuable feedback, questions and proposals for amendments.

This communication summarises the main issues raised in the public consultation and the principal amendments to be made to the CROE as a result.

2 Comments received in the public consultation

Comments mostly focused on four aspects:

1 See CPMI-IOSCO (June 2016), "Guidance on cyber resilience for financial market infrastructures".
2 See CPSS-IOSCO (April 2012), "Principles for financial market infrastructures".

- the level of the expectations' prescriptiveness;
- the three levels of maturity and how these correspond to other international cybersecurity frameworks that also have maturity models;
- the process for oversight assessments against the CROE;
- the need for harmonisation across different jurisdictions and among regulators to reduce the fragmentation of regulatory expectations and facilitate oversight convergence.

2.1 The level of the expectations' prescriptiveness

A number of respondents were concerned that the expectations were overly prescriptive. To address these concerns, the updated CROE acknowledges that as FMIs implement the expectations, at times they will do so in different ways. In cases where the FMIs do not meet the prescribed expectation, they should provide an explanation to the relevant overseer of how they meet the objective of the underlying expectation. The *meet or explain* principle provides FMIs with a degree of flexibility in their approach to enhancing their cyber resilience capabilities, given that FMIs are heterogeneous and will differ in size, organisational and operating structure, business model and infrastructure set-up. Consequently, it is feasible that FMIs may meet the underlying expectations by using different processes, technologies and methodologies.

2.2 The three levels of maturity

A number of respondents highlighted that several international cybersecurity frameworks already incorporate maturity models, and therefore, further clarity was sought on how the three levels of maturity set out in the CROE correspond to other international frameworks, which FMIs may have already adopted.

From the outset, the CROE indicates that *"the FMI should use leading international, national and industry-level standards, guidelines or recommendations (e.g. NIST, COBIT 5 and ISO/IEC 27000, etc.), reflecting current industry best practices in managing cyber threats, as a benchmark for designing its cyber resilience framework and incorporating the most effective cyber resilience solutions"* and *"The FMI should use maturity models and define relevant metrics to assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework through independent compliance programmes and audits carried out by qualified staff on a regular basis."*

Furthermore, while developing the CROE, the authors considered existing international guidance documents and frameworks: the NIST Cybersecurity Framework, ISO/IEC 27002, COBIT 5, the Information Security Forum's Standard of Good Practice for Information Security and the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool were used as a

basis, in particular. Although FMIs may use maturity models from these or other international standards and frameworks for their internal purposes, the levels of expectation set out in the CROE are intended to provide the benchmark for overseers to determine their FMIs' cyber resilience capabilities against the Guidance.

However, to provide further clarity on this issue, the updated CROE has now replaced all references to *levels of maturity* with *levels of expectation*. The cyber threat landscape is constantly evolving and reaching higher levels of sophistication. In the light of this, FMIs should make further efforts to adapt, evolve and improve their cyber resilience capabilities. To address the idea of continuous adaptation, evolution and improvement, the CROE sets out levels of expectation which provide the overseers and FMIs with a benchmark against which they can evaluate the FMIs' current level of cyber resilience, measure progression and establish priority areas for improvement. The *levels of expectation* set out the state of cyber resilience that overseers expect their FMIs to reach and maintain, and are not a reflection of the level of the FMI's maturity nor designed to replace other existing maturity models integrated into international cybersecurity frameworks.

Finally, the initial CROE had three levels of maturity or expectation: *baseline*, *intermediate* and *advanced*. Following the public consultation, the authors felt that the essence of these three levels of expectation is the continuous improvement and maturing on the part of the FMI. Indeed, the levels of expectation are not designed to establish static requirements and an end state of cyber resilience, which risks creating a culture of compliance. Rather, FMIs are expected to be constantly evolving, advancing and innovating in the light of the continuously evolving cyber threat landscape. Therefore, the levels of expectation are now referred to as: *evolving*, *advancing* and *innovating*.

2.3 Process for oversight assessments against the CROE

Several respondents sought further clarity on how the CROE would be used to conduct oversight assessments of the relevant FMIs. A key cornerstone of the CROE is that it will be used on a regular basis to assess FMIs. As FMIs embed the expectations across their enterprises and strive to achieve the desired outcomes, there is a necessity to conduct regular oversight assessments to measure the effectiveness of their cyber resilience capabilities and their continuous evolution, advancement and innovation.

The Eurosystem oversight function has reflected on the assessment process and the lead overseer will communicate this bilaterally to the respective FMIs.

2.4 Harmonisation

A number of respondents stressed the importance of harmonising the expectations with other international frameworks and engaging with other key regulators to agree on and standardise a common framework and assessment process, thereby

reducing the fragmentation of regulatory expectations, facilitating oversight convergence and reducing the potential burden of additional costs on FMIs.

The Guidance, published in June 2016, is applicable to FMIs around the world and provides a harmonised approach for them to improve their cyber resilience capabilities. Building on this, the CROE sets out concrete expectations on how payment systems and T2S (and other types of FMIs, if they wish) can operationalise the Guidance in the euro area. The concrete expectations, therefore, already provide a harmonised approach for a significant number of FMIs in the euro area. Notwithstanding this, the CROE has been drafted for all types of FMIs and the ECB stands ready to explain its application to other regulators around the world in pursuit of achieving increased harmonisation.

The CROE will be applied for the oversight of payment systems and T2S, while national authorities responsible for the oversight of clearing and settlement systems, i.e. securities settlement systems (SSSs), central securities depositories (CSDs) and central counterparties (CCPs), are free to apply the CROE should they wish to do so. Several of the aforementioned clearing and settlement systems are cross-border group entities that operate in multiple jurisdictions and are subject to oversight by a number of different authorities. It is therefore important in such cases for the CROE to be applied consistently to avoid possible fragmented application and interpretations, which may result in inconsistencies, diverging level playing fields, a fragmentation of expectations on FMIs operating throughout the different jurisdictions, and diverging and conflicting assessments of the same cyber resilience capabilities.

In this regard, the different relevant authorities are encouraged to align the levels of expectation for their respective FMIs to avoid potential inconsistencies in the assessment of those levels. The different authorities and overseers should strive to take a coordinated and aligned approach when carrying out their assessments, and establish or utilise existing cooperative structures. Ensuring a consistent and aligned approach will also allow the FMI to take the right steps and make the right investments to further enhance its cyber resilience capabilities.

3 Other comments received in the public consultation

Aside from the points above, the public consultation gave rise to a number of comments and requests for amendments to, and deletions and clarifications of specific expectations. The authors reviewed each comment and request in detail and where further clarity could be provided, the appropriate alterations were made to the specific expectations.