EUROPEAN CENTRAL BANK

EUROSYSTEM

DIRECTORATE GENERAL
MARKET INFRASTRUCTURE AND PAYMENTS

ECB-PUBLIC

05 June 2018

TEMPLATE: COMMENTS ON THE

DRAFT "CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES"

Contact details (will not be published)	Ms.	Chiara Bergamaschi
	Chiara.bergamaschi@eachccp.eu	
	+32 (0) 22061261	
☐	The comments provided should NOT be published	

The table below shall serve as a template for collecting comments in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**.
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on (i.e. one row for each issue).
- If needed for the provision of further comments, please replicate page 3.

The assessment form consists of the four items which are suggested to be filled as follows:

- **Originator:** Name of the originator and ISO code of the country of the originator (i.e. NAME (AT/BE/BG/...))
- **Issue** (states the topic concerned): General comment, Specific comment on an Expectation, Request for definition, and Request for clarification of issue or terminology
- **Comment:** Suggestion for amendment, clarification or deletion
- **Reasoning:** Short statement why the comment should be taken on board

Please send your comments to ECB-Oversight-consultations@ecb.europa.eu by 05 June 2018.

Originator:

Name of the originator (i.e. name of the company or association)	European Association of CCP Clearing Houses (EACH)	ISO code of the country of the originator	BE

EACH comments on the draft Cyber Resilience Oversight Expectations for Financial Market Infrastructures

Issue	Comment	Reasoning
General comment	Clarification	EACH welcomes the opportunity to provide input to the draft ECB cyber resilience oversight expectations (CROE). We agree that a continuous work on cyber resilience capabilities will limit the potential risks raising from cyber threats. We welcomed the publication in June 2016 of the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures. We believe that the ECB provide a good guidance on cyber resilience of FMIs. However, it would be helpful to have more objective-based requirements that are not overly prescriptive. This approach would provide FMIs the necessary flexibility to achieve the same objectives with types of controls and measures that are not specifically prescribed. We believe such flexibility in approach would be particularly important considering that financial market infrastructures' (FMIs) are very different from each other in the services they offer and the markets they serve. We concur with the view that CROE should be considered as a set of practices to help comply with the CPMI-IOSCO guidance and not a strict checklist to be compliant with. We would like to emphasise the important of the principle of proportionality. We believe that authorities, following their discretion and judgement, should determine the level of maturity (baseline, intermediate or advanced level) required by the FMIs. This would mirror the differences between EU CCPs in term of size, volume and products cleared.

Governance - Cyber resilience strategy and framework – par 2.1.2.1.	Amendment	EACH notes that the ECB CROE propose very detailed requirements in terms of governance expectations which go far beyond the CPMI-IOSCO Guidance and do not allow to accommodate different size and organizational structures of FMIs. In particular we share the principle that the Board and the full FMI senior management shall actively participate to the creation of a cyber resilience culture. However, it should be noted that the CPMI-IOSCO Guidance also requires that the Cyber Resilience Framework shall be supported by defined roles and responsibilities of the Board and the management. In this regard we believe that the requirement to establish 'cross-disciplinary steering committee' could create uncertainty in terms of responsibilities and interactions with the Board and the Chief Information Security Officer (CISO). We would rather welcome an approach where by the CISO according to its own responsibility and task coordinates the participation of other business units to the development of the cyber resilience framework that should be finally endorsed by the Board. Therefore, EACH suggest removing the reference to the '*cross-disciplinary steering committee'* from paragraph 1 of the CROE.
Governance - Cyber resilience strategy and framework – par 2.1.2.1.	Clarification	EACH believes that the cyber resilience strategy needs to be integrated in an overall strategy of operational risk management. Aligning cyber risks using an approach of proportionality allows encouraging responsible boards to arrive at a balanced, risk-aware management approach. This means that the cyber resilience strategy has to be both holistic and adaptive to threat landscape and organisational-specific values and weaknesses. More concretely, the strategy needs to value the relative size of an organization to enable a risk-balance approach. Consequently, there should be no 'one-size-fits-all' approach but an adaptive strategy which allows for cyber resilience to be managed proportionally to the risk appetite, situation and environment. This certainly requires a two-prong direction: minimum cyber resilience based on threat profile with a scalable incremental set of resilience controls to reflect lower risk appetite.

Governance - Role of the board and senior management - 2.1.2.2. Par. 20	Amendment	With regard to the role of CISO we share the view that it is a key organizational role for cyber resilience. We believe that the FMI should retain the necessary flexibility to determine how to incorporate the CISO in its own organizational structure. This should be without prejudice to the fact that the CISO has sufficient 'authority, independence, resources and access to the Board' as provided in the CPMI-IOSCO Guidance. Therefore, we suggest amending paragraph 20 as follows: *20. The Board and senior management should ensure that a senior executive (e.g. Chief Information Security Officer) is responsible and accountable for the implementation of the cyber resilience strategy and framework at the enterprise level. The senior executive should be independent, possess the appropriate balance of skills, knowledge and experience, have sufficient resources and* ***direct access*** *~~report directly~~ to the Board. For further clarification on the possible roles and responsibilities of such a Senior Executive, please refer to Annex 3.*
Identification – par 2.2	Clarification	While other industries are right to focus identification efforts on assets, we believe that FMIs should have a different and specific focus on availability and avoiding tamper or disruption. For FMIs, the threat of 'lobbing a grenade' is much more relevant and the choice of specific asset to target is less important than disrupting any of many interconnected links that would result in outage or instability. To that end, we believe that identification efforts should be focused on identifying threat actors and categories, tools, and methods so defences may be properly positioned and tested. We also believe that a clearer guidance should be provided on the level of coordination required between an FMI and external stakeholders. For example, information-sharing with stakeholders may be inappropriate in certain cases (where this involves the disclosure of confidential or competitively-sensitive information and may therefore lead to additional risk exposures for the FMI).

Protection -par 2.3.2.1.2.	Amendment	As FMIs have different levels of maturity, we welcome that the level of ICT controls should be handled proportional to the risk-balanced model. Different FMIs may have varying degrees of maturity, driven by different market sizes, market conditions and threat exposures (e.g. according to their attractiveness to threat actors). We would also like to highlight that the Network & Infrastructure Management section on requirements for FMIs to implement intrusion detection/prevention systems seem overly prescriptive and we believe that similar level of controls can be obtained with alternative methods such as 'access gateway/jump box' and connecting these to virtualisation solutions such as Citrix. This would make it impossible to build external attacks as solutions are limited at the source.
Detection – par 2.4	Clarification	Proper detection of an attack needs FMIs to understand the cyber security kill chain. In addition to the motivation of an attacker (group), it is critical to understand the typical attack vectors, indicators for attack pre-cursors (not only indicators of compromise) and long-term attack indicators. Preparedness (cyber resilience) rules need to be triggered when pre-cursors are being detected, as actual attack vectors might only occur when defences have already been breached. We therefore welcome an early warning system.

Response and Recovery – par 2.5 par 14	Amendment	We welcome the ECB's effort to clarify that notwithstanding the capability to resume critical operations within two hours the FMI should exercise judgment in effecting resumption. We recognise the value in having a soft target time to aim for, but given the nuances, potential complexities and specifics of each individual market and incident (many of which cannot be predicted or planned for), it may not be in the best interests of the fairness, orderliness and stability of the market to be forced to resume operations within a deadline if not completely ready to do so. As such, the FMI needs to use its best judgement as to the optimal (and safest) time to bring markets and clearing systems back into operation given the systemic importance of them. We also believe that a coordinated approach and information sharing among different stakeholders and market authorities is needed before resuming operation. In addition, in case of cyber-attacks that undermine the integrity of data, the FMI shall be allowed sufficient time to carry on the problem determination phase before the resumption of its critical function, in order to be sure that the re-start of operations is based on the last consistent set of data. Therefore, we suggest the following amendment to the paragraph below: *"The FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, FMIs should* ***undertake careful problem detection*** *and exercise judgment* ***(in agreement with competent authorities and relevant stakeholders where the case maybe)*** *in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account the fact that completion of settlement by the end of day is crucial."*
Response and Recovery –	Clarification	We would welcome clarification on the meaning of 'independent reconciliation of participant position'.
Situational Awareness – par 2.7.2.2.	Clarification	EACH notes that it is prescribed that the FMIs should develop an in-house threat intelligence capability. We support the objective of such requirement and we would like to note that there are specialised service providers in such area and could be in a better position to offer this service, especially when it comes to FMIs of limited

Annex 3	Deletion	As per the comment above we believe that ANNEX 3 should be revised in order also to cater for different size and organizational model of FMIs (such groups). In particular, organizational models such as the one outlined in the footnote n. 5 whereby the CISO remains in the technology organizational area while ensuring proper information flow and access to the Board shall be allowed under the CROE. In line with this, we suggest deleting point 2(b) and point 4 of ANNEX 3, as keeping it would effectively prevent the existence of the organizational models such as the one in footnote n. 5.