EUROPEAN CENTRAL BANK
EUROSYSTEM

DIRECTORATE GENERAL
MARKET INFRASTRUCTURE AND PAYMENTS

ECB-PUBLIC

10 April 2018

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

Contact details (will not be published)	Ms.	Eve Chen (Tzu-Yu)
	echen@lseg.com	
	+44 (0)7896571089	
☐	The comments provided should NOT be published	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)	London Stock Exchange Group	ISO code of the country of the originator	UK

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

Issue	Comment	Reasons
Overall	Amendment	We believe that the ECB provides a good guidance on cyber resilience of FMIs. We welcome the ECB's approach to leverage off the existing international guidance documents and frameworks whilst developing the CROE. We consider that the consistency and consideration of existing requirements would be key for regulatory compliance. In our view, it is crucial to ensure that an internationally consistent approach is taken in order to mitigate any regulatory arbitrage and to ensure strong cyber security requirements across industries. A globally harmonised approach would allow companies with global reach to operate across borders with predictability and clarity of standards. It would ensure efficient use of time and resources within the businesses. However, it would be helpful to have more objective-based requirements that are not overly prescriptive as illustrated below. This approach would provide FMIs flexibility to achieve same objectives with types of controls and measures that are not specifically prescribed. We would also like to note that, considering the existing arrangement of information submission to NCAs, additional and excessive information submission would increase the burden on institutions on an operational level. We would therefore encourage any NCAs implementing these guidelines to take into account existing processes and recent reviews of cyber security exercises.

2.3.2.1.2. Network & Infrastructure Management:	Amendment	The requirement on implementing intrusion detection/prevention systems (e.g. IDS/IPS) and endpoint security solutions (e.g. antivirus, firewall, and HIDS/HIPS) seem quite prescriptive and its objectives could be fulfilled with a more objective-based approach. We believe that similar level of controls could be obtained by using "access gateway/jump box" and connecting these to virtualisation solutions such as Citrix. Therefore, it would be impossible to build external attacks as solutions are limited at the source. We would suggest allowing alternatives to this requirement as long as the objectives are fulfilled.
2.7.2.2. Information sharing	Amendment	The requirement for FMIs to develop an in-house threat intelligence capability should be treated with caution. We support the objective that this requirement is trying to achieve but we would like to note that specific service providers specialised in such area might be in a better position to offer this expertise, especially when it comes to FMIs of limited size. We would therefore suggest focussing on the implementation by the FMI and allow the FMI to use external intelligence to a certain extent.

2.1.2.1. Cyber resilience strategy and framework	Amendment	We note that CROE proposes very detailed requirements in terms of governance expectations which go beyond the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures ("CPMI-IOSCO Guidance") and thus insufficient flexibility to accommodate different sizes and organisational structures of FMIs. We support the principle that the board and the 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 Cyber Resilience Framework shall be supported by defined roles and responsibilities of the board and the management. In this regard we see 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 Office ("CISO"). We would welcome an approach under which, the CISO should coordinate the participation of other business units to the development of the cyber resilience framework to be endorsed by the Board. Therefore we suggest removing the reference to the "*cross-disciplinary steering committee*" from paragraph 1 of the CROE.

2.1.2.2. Role of the board and senior management	Amendment	We note that CROE proposes very detailed requirements in terms of governance expectations which go beyond the CPMI-IOSCO Guidance and might thus not provide sufficient flexibility to accommodate different sizes and organisational structures of FMIs. We share the view that the CISO is a key organisational role for cyber resilience; however FMIs should retain the necessary flexibility to define its set-up dependent on its own organisational structure, particularly in terms of internal reports. We would therefore suggest to amend 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.* This should be without prejudice to the fact that the CISO has sufficient "authority, independence, resources and access to the board" as provided in CPMI-IOSCO Guidance (§§2.3.4).

2.5.2.1. Cyber resilience incident management	Amendment	We welcome the ECB's approach under paragraph 14 which clarifies that notwithstanding the capability to resume critical operation within two hours the FMI should exercise judgment in effecting resumption. This is crucial in case of cyber attacks which could generate a systemic effect, despite the triggering event affects only one entity. In this case 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, FMIs 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 operation is based on last consistent set of data. A forced two hour resumption period could potentially exacerbate the situation because if the system's integrity is compromised then successful recovery within two hours may not necessarily mean that the restored system is fit for purpose. In addition, with reference to the requirement to complete settlement by the end of the day, we consider that, in the case where cyber-attacks having systemic impact, the decision to resume settlement operation should be the result of a joint assessment performed by the FMIs, participants and competent authorities jointly. 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)*** *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."*

2.5.2.2. Data integrity	Clarification	We would welcome clarification on the definition of "independent reconciliation of participant position".
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 organisational structure of FMIs. In particular organisational model such as the one outlined in the footnote n. 5 whereby the CISO remains in the technology organisational area while ensuring adequate information flow and access to the Board shall be allowed indirectly, through the CROE. In this view we suggest to delete point. 2(b) and point 4 of the Annex.