EUROPEAN CENTRAL BANK
EUROSYSTEM

DIRECTORATE GENERAL
MARKET INFRASTRUCTURE AND PAYMENTS

ECB-PUBLIC

5 June 2018

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

Contact details (will not be published)	Ms.	Alexandra Maniati, Senior Policy Adviser, Cybersecurity & Social Affairs
	a.maniati@ebf.eu and s.tringali@ebf.eu	
	+32 2 508 37 36	
☐	The comments provided should NOT be published	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 Banking Federation	ISO code of the country of the originator	BE

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

Issue	Comment	Reasoning
General comment	Amendment	Due to the amount of details within the consultation paper, the creation of an executive summary, highlighting the key points, would be useful for complying with the Guidance requirements.
General comment	Clarification	We believe that a clarification of the nature of controls on the FMI's participants and counterparties should be included in an FMI's cyber risk documentation.
Request for addition (1.2.)	Amendment	In addition to the creation of a traceability matrix between the CROE standards and the FMIs' existing policies, we would welcome the Guidance to describe the FMIs' tools to demonstrate their compliance.
Specific comment on maturity models (1.2., last paragraph)	Amendment	In order to avoid framework fragmentation, we propose that the maturity models set out in the CROE are imposed as the unique benchmark for internal purposes.
Request for addition (2.1.2.1., 9th paragraph)	Amendment	For avoidance of doubt, we suggest adding the following sentence ''FMIs must, of course, comply with any applicable mandatory requirements issued by public authorities to which they are subject.''
Request for replacement (2.3.2.1.1., 5th paragraph)	Clarification	In order to be clearer, we suggest that the word ''redundancy'' is replaced by the phrase ''back-up.''
Request for addition (2.3.2.1.4.)	Amendment	At the end of this issue, we propose to add a paragraph number 54 (or 53a to avoid renumbering subsequent paragraphs) stating that the obligation to guarantee that all the FMIs systems remain consistently up to date (i.e. existing paragraph 55) is extended also to those FMIs that are subjected only to baseline requirements.

Request for addition (2.3.2.2.1. - 58b)	Amendment	Given that not all national jurisdictions may allow background checks or behavior monitoring for employees on a periodic basis, as required by the CPMI-IOSCO guidelines, we propose that an amendment is made to reflect that these checks may be conducted without prejudice to related national legislation.
Request for addition (2.3.2.2.1. - 63)	Amendment	The same as the previous comment on adherence to national legislation.
Request for replacement (2.4.2. - 20)	Amendment	Due to the potential risks involved in implementing such deception mechanisms on production systems, we suggest the replacement of paragraph 20 by a more generic requirement for processes and testing to detect malicious activity.
Request for clarification/ addition (2.6.2., 4th paragraph)	Clarification	As regards cyber resilience tests for FMIs, which are carried out by either internal or external independent third parties, a clear distinction between security testing programs and independent assessments is considered necessary.