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Contact details (will not be published)	Mr.	Andre Vink
	a.vink@ebaclearing.eu	
	0032 2 475 782 682	
☐	The comments provided should NOT be published	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)	ABE CLEARING S.A.S. à capital variable (EBA CLEARING)	ISO code of the country of the originator	EU

EBA CLEARING's comments on the draft Cyber Resilience Oversight Expectations for Financial Market Infrastructures

Issue	Comment	Reasoning
1. General Comment on the additional volume of controls set by the CROE as compare to the Guidance	Clarification	The CROE is not only implementing the Guidance but 'operationalising' the requirements set out by the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (the "Guidance") based also on other international standards or frameworks. As a result, the CROE increases the number of controls as compared to the Guidance by a factor of five (69 controls for the Guidance to over 332 controls for the CROE). These additional controls considerably extend and redesign the set of requirements against which FMIs' preparatory works, ongoing since June 2016, were based; the CROE's numerous new controls once adopted will need to be analysed and compared to the existing plans to improve cyber resilience frameworks of FMIs and, as the case maybe, those plans will need to be adjusted taking into account the unusual level of details set forth by the CROE. Such an exercise is even more a delicate process since, as underlined by the CROE, strengthening cyber resilience requires FMIs to outreach to participants and other stakeholders such as Critical Service Providers, which could delay reaching a timely compliance with the Guidance. As regards assurance by Critical Service Providers, EBA CLEARING is of the strong opinion that a standardised methodology should be applied under the control of the supervisory / regulatory / oversight authorities of those CSP's (including for reasons of security, and see also below).

2. General Comment on the absence of harmonised timeline for compliance with the CROE/ adoption by authorities	Clarification	The CROE refers to the timelines set by the Guidance for overseers to develop an oversight approach to assess their FMIs and for the FMIs to comply with it. Yet, the CROE, while going beyond the mere transposition of the Guidance's controls, lacks a timeline indicating by when FMIs, in particular but not necessarily only those overseen by the Eurosystem, would be assessed against such CROE and are expected to comply with them. A harmonised transition period to comply with these requirements would enable to attain the objectives of the CROE in a coordinated manner, which would be more efficient considering also the need for FMIs to outreach to a number of other stakeholders which may be the same across FMIs due to the extensive interconnections underlined in the CROE.
3. General Comment on link with the assessment methodology	Clarification	As far as payment systems are concerned, the CROE purports to set clear criteria against which the overseers assess the FMIs, and it is further stated in section 1.4.2 of the CROE that far from a mere check list, it is to be seen as "a set of practices that can contribute to compliance with the Guidance" as will remain to be clarified by the relevant overseer for each system individually. The link between oversight requirements and the correlated rating for observance / compliance and the interpretation of the oversight expectations by each overseer for each system would merit clarification. Where judgement will be applied by the respective overseers – both in relation to specific expectations and in relation to the expectation for continuous improvement --, this may have an impact on the level of predictability of requirements and related costs / investment needs for the FMI.

4. General Comment on the role of Critical Service Providers (CSP)	Clarification	In settings where an FMI and its participants have chosen to rely, for all or part of the critical services, on providers in the market of the highest repute, EBA CLEARING advocates for avoiding a duplication or multiplication of assessments both by FMIs and by regulatory / supervisory / oversight authorities. In addition, limitations on sharing of information by critical service providers with their, potentially multiple, "FMI customers" should be recognised, both in principle and in practice. An aspect also not explicitly covered in the CROE is whether the Eurosystem intends to extend the principles set out in the CROE for FMIs to critical service providers (CSP) (currently covered by Annex F of the PFMI), and whether CSP's are expected to demonstrate that they meet the requirements from the CROE as well (such as implementing the (relevant) controls from the 119 controls set under "identification", "detection" or "protection", and such as putting in place appropriate detection mechanisms as per section 2.4.1, #20). Should this be the case, EBA CLEARING strongly advocates for a standardised methodology under the control of the CSP's competent authorities. FMIs should continue to rely on oversight arrangements for CSPs by competent authorities within the EUROSYSTEM (alone or in cooperation) which are already in place, similar as for the provision of settlement services to ancillary systems (section 2.3.2.3, # 72 of the CROE). 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. Further, the same regime should be applied for the providers of critical services that are overseen by competent authorities, regardless of the type of critical services.

5. Section 1.4 General Comment on the requirements by type of FMI	Clarification	The CROE defines three levels of cyber resilience maturity against which FMIs should be "benchmarked" where the Guidance defines none and while acknowledging that maturity models based on international standards exist and might be used by FMIs in their preparations for compliance with the Guidance. The CROE do not give the rationale why this maturity model has been preferred. The introduction of new elements as part of the operationalisation of the Guidance for the oversight of FMIs by the Eurosystem may lead to a risk of creating an uneven playing field for FMIs. With respects to payment systems (section 1.4.2), the CROE set the expectation that they are expected to reach and maintain a given level of maturity at a minimum and yet to take also active steps over time to attain the next level of maturity. It is, however, unclear what aspiring to the next maturity level over time will mean. We believe the path to the next level of maturity is vague and subsequent steps and related cost should be considered against potential risk benefits. The CROE should enable a payment system to determine upfront what requirements are or might over an ascertainable period of time be applicable to it to avoid creating uncertainties for concerned entities and their plans to reach compliance with the relevant expectations as well as for their participants and other interconnected stakeholders. The proposed coupling of an assigned minimum per category of payment systems with a possible aspiration to the next maturity level could accrue the risk of uneven playing field if the CROE are not applied consistently to all types and size of payment systems. The fourth paragraph of the section 1.4.2 referring to the CROE as rather "a set of practices that "*can"* contribute to compliance with the Guidance" further raises the question on the exact nature of these "oversight expectations" for FMIs subject to them, especially when alternate arrangements, which can be equally effective, may already be in place. Clarification on this point would thus be wishful. In particular, the document goes into a level of details (e.g. providing guidance on slogans to be used to convey leadership and vision on cyber-resilience) which is not usual in oversight expectations risking to create unbalance how, by comparison, compliance with other requirements in scope of the principles for FMIs has to be attained and assessed.

6. Section 1.4.1 General Comment	Amendment	As a minor perception comment, colour codes of the maturity levels define as baseline (green) and advanced(red) should be inverted or replaced by other colours reflecting the gradation towards the advanced level (e.g. bronze, silver, gold or similar).
7. Section 2.1 Governance	Clarification	#28/29: The CROE foresees that 'senior management should ensure that it has a programme for continuing cyber resilience training and skills development for all staff. This training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security) and emerging issues.' As a rule, the training programme and its content shall overall be proportionate and relevant to the roles of the trainees and their existing skills. Proportionality should not be reserved to additional specialist training. For instance, although Board members shall be involved in cyber topics e.g. by means of regular workshops and incidents responses, involving them in specific cyber topics like phishing, spear phishing, social engineering, and mobile security training shall be commensurate to their role and existing skills taking into account e.g. training followed on such topics outside the FMI context. This aspect seems to be missing from the abovementioned points of the CROE. Further, a Board needs diversity in skillsets well beyond 'cyber' to function well, and an emphasis on cyber that is disproportionate could cause other skills to wither.

8. Response and Recovery controls	Clarification & Amendment	#29: Under this section of the CROE, it is stated that 'the FMI should consider having a data-sharing agreement with third parties and/or other stakeholders in order to obtain uncorrupted data from them for recovering its business operations in a timely manner and with accurate data'. EBA CLEARING considers that this requirement is a rather ambitious expectation for FMI involving numerous parties with different profiles and background such as retail payment systems. The consideration that there may be limitations for FMIs to obtain from third parties to commit to such agreements should be better reflected in the CROE. The terminology of "third parties and/or other stakeholders" used in this section is less precise than the one use by the Guidance of "third parties or participants" which would be clearer.
9. Section 2.7 Situational Awareness	Amendment	Section 2.7 of the CROE requires FMIs to participate in multilateral information sharing arrangements with direct and external stakeholders and build capabilities to analyse information security incidents experienced by other organisations, including types of incident and origin of attacks, target of attacks, preceding threat events and frequency of occurrence and determine the potential risk these pose to the FMI. EBA CLEARING has strong reservations against the sharing of this type of highly sensitive information in an unstructured way. EBA CLEARING would rather see this type of information collected and shared in a centralised and controlled environment, for example at a competent European authority, where information security is safeguarded and can be more efficiently made available. EBA CLEARING notes that FMIs appear to be given the most active role in such multilateral information-sharing arrangements while the role that authorities could play remains vague and should be made more explicit.

10. Section 2.7 Situational Awareness	Amendment	#24. The CROE requires that the 'FMI should develop an in-house threat intelligence capability (including personnel, infrastructure and training) which sources and stores internal and external threat and vulnerability information, analyses this information, and disseminates it to the relevant stakeholders in the ecosystem in a prompt manner, so as to facilitate early response and risk mitigation by the stakeholders. The FMI should, as far as possible, automate this process.' EBA CLEARING sees the development of such a capability in house by every FMI as an inefficient solution and a misuse of resources. We would rather see a centralised solution managed by authorities at European level against a commonly defined standard as example MISP, STIX and TAXII.
11. Section 2.8 Learning and Evolving	Clarification	# 13: To give an example where the CROE introduces requirements for which it is not clear how the assessment will be applied, we can refer to the requirement for the FMIs 'to use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to predict potential future cyber events and trends, and proactively take the appropriate measures to improve its cyber resilience capabilities'. It is unclear from the CROE what types of efforts would be good enough for the FMI to meet the requirement of this control # 13.