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| **Contact details (will not be published)** | Ms. | Marija Kozica |
| | marija.kozica@deutsche-boerse.com | |
| | +49 (0) 69 211 17178 | |
| ☐ | The comments provided should NOT be published | |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)** | DEUTSCHE BÖRSE GROUP | ISO code of the country of the originator | DE |

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

| Issue | Comment | Reasoning |
|---|---|---|
| General comment – Implementation period (1.2) | Amendment | While the Cyber Resilience Oversight Expectations (CROE) refer under Section 1.2. to the immediate applicability of the underlying CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, no information on the foreseen implementation period for the CROE, once they have been finalized and entered into force, has been provided.<br><br>In order to ensure appropriate implementation of the specifying CROE an implementation period should be determined. We consider a grace period of at least 24 months until the CROE are being considered within the regular oversight and supervisory activities of the Eurosystem as appropriate and suggest to explicitly include the implementation period within the CROE. |
| General comment – Alignment with NCAs (1.3.) | Clarification | The CROE will be applied for the oversight of payment systems and T2S, whereas national competent authorities (NCAs) responsible for the oversight of clearing and settlement systems, i.e. SSSs, CSDs and CCPs, are free to apply the CROE as well as to set the maturity levels they expect the respective FMI under national oversight to reach.<br><br>Although DBG generally support this approach to leave sufficient room for national particularities, we would like to expresses our concern that a fragmented application and interpretation of the CROE regarding maturity levels might result in inconsistencies, diverging level playing fields and a fragmentation of expectations on FMIs operating throughout different jurisdictions. As FMIs often operate within groups encompassing more than one FMI providing services cross-border, an inconsistent application of the CROE might lead to conflicting as well as diverging assessments of same cyber resilience frameworks.<br><br>We would like to encourage the ECB to further align the CROE with NCAs in order to avoid potential inconsistencies on the assessment of maturity levels and setting of expected maturity levels. We support a coordinated and aligned regulatory guidance approach rather than a detached simultaneous development of different oversight expectations as this would increase fragmentation of regulatory guidance, thus, inadvertently foster risk and financial instability in the ecosystem. |

| | | |
|---|---|---|
| General comment – Determination of expectations on maturity levels (1.3.) | Clarification | According to Section 1.3. PIRPS and ORPS are expected to reach a baseline level of maturity, whereas the expected maturity level for SIPS and T2S is intermediate.<br><br>As the central platform for securities settlement, T2S plays a key role for the stability of the financial system and FMI ecosystem and can become a single point of failure. In the absence of criteria used to determine the expected maturity level, we are not able to comprehend the expected maturity level.<br><br>We consider the provision of key criteria used for determining the expected maturity level of an FMI or type of FMI as important in order to enable FMIs to assess their potentially expected maturity level and provide guidance to NCAs potentially adopting the CROE. By providing the underlying criteria, FMIs could be able to provide valuable feedback on whether T2S, as the key platform for securities settlement within Europe, should be expected to reach an intermediate level or whether an advanced maturity level would be more appropriate.<br><br>We suggest to include the key consideration underlying ECB's expectation on the respective maturity levels to be reached by PRIPS, ORPS, SIPS and T2S into the CROE. |
| General comment – Legal basis (1.3.) | Amendment | As outlined under Section 1.3, the Eurosystem will apply the CROE for oversight of FMIs and T2S.<br><br>In order to be able to determine the entities in scope of the CROE precisely, we kindly ask to include reference to the legal basis underlying and determining the Eurosystem's oversight responsibilities. |
| General comment – Definition of FMI | Clarification | The CROE will be applied to FMIs of the Eurosystem, whereas PIRPS, ORPS, SIPS and T2S are named as being concretely in scope. NCAs are free to apply the CROE to further FMIs under their supervision.<br><br>While the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures contains a definition of FMI in the glossary, no definition of FMI is anchored in European legislation so far. As a clear definition of the term "Financial Market Infrastructure" is necessary to define the scope of entities potentially in scope, we demand clarification on what is to be considered "FMI". |

| | | |
|---|---|---|
| Specific comment - Levels of maturity (1.4.1.) | Amendment | As outlined under Section 1.4.1, the concept of maturity levels has been chosen to follow the idea of continuous adoption, evolution and improvement. Nevertheless, by adopting selected structural elements of existing standards (e.g. NIST) while introducing new conceptual elements, inconsistencies may arise. The three maturity levels (baseline, intermediate, advanced) do not necessarily build-up on each other logically as, for comparison, COBIT does with process maturity levels. FMIs might cover some elements from each of the three levels simultaneously (e.g. when interconnected with other FMIs but not having continuous improvement internally). This might lead to inconsistent maturity ratings by different stakeholders.<br><br>While we generally support that the CROE are structured following closely already well established standards, we recommend to rearranging maturity levels such that they reflect a continuous adoption, evolution and improvement as intended. |
| Specific comment – Composition of steering committee (2.1.2.) | Clarification | According to para. 1 of Section 2.1.2. the FMI shall establish an "internal, cross-disciplinary steering committee" comprising of participants from senior management and different business units.<br><br>As particularly within a group of entities central functions as legal and HR are often being outsourced to an affiliated company, we suggest to explicitly allow for group internal but legal entity (i.e. the FMI in scope) external functions and employees to participate in the internal steering committee. Although consisting of group-internal but legal entity external participants, the steering committee can act as an internal body to the best interests of the FMI.<br><br>Please clarify whether our understanding outlined above corresponds to the named oversight expectation. |
| Specific comment – Governance & Board Expertise (2.1.2) | Clarification | Under Section 2.1.2.2 para. 19 et seq. the Board is expected to have "the appropriate balance of skills, knowledge and experience to understand and assess cyber risk facing the FMI".<br><br>We suggest cyber-risk expertise should be either available by a board member with adequate experience, or by experienced staff / organization(s) reporting to the Board with adequate cyber-risk and cyber-security expertise (providing advice to the Board). |

| | | |
|---|---|---|
| Specific comment – Review of the cyber resilience framework (2.1.2.) | Amendment | Para. 11 of Section 2.1.2. requires the FMI's Board to review and update the cyber resilience framework at least annually.<br><br>While an annual review of the FMI's cyber resilience framework is reasonable, a mandatory annual update might be contradicting the framework's strategic long-term perspective and create an unnecessary burden to update the framework although not considered relevant. We therefore suggest re-phrasing the respective expectation accordingly to limit the mandatory update of the cyber resilience framework to when considered necessary. |
| Specific comment on expectation – Documentation (2.1.2.2 and 2.5.2.4) | Clarification | According to para. 18 of Section 2.1.2.2. the respective FMI's Board shall approve the cyber resilience strategy and framework while para. 47 of Section 2.5.2.4. requires the implementation of a forensic readiness policy approved by the board.<br><br>Neither the cyber resilience strategy and framework nor a forensic readiness policy do necessarily have to constitute dedicated and separate documents to be effective but can rather form parts of an overarching IS policy and cyber security framework. Similarly, a Cyber Code of Conduct, as demanded under para. 36 of Section 2.1.2.2, should not mandatorily be specified within a separate document. Specifying details and dedicated measures can be set complementary through adequate standards and procedures.<br><br>In order to avoid isolation treatment of different elements of cyber security, we suggest to explicitly clarifying that a FMI's cyber resilience strategy and framework as well as measures ensuring forensic readiness can be included in other overarching frameworks and approved by the board as such. |
| Request for definition – "Process" vs "Business process" (2.2.2.) | Clarification | Para. 1 of Section 2.2.2. requires the identification and documentation of, among others, "processes" whereas under para. 2 ibidem FMIs shall identify and document "business processes".<br><br>Please provide clarification on the difference between "processes" and "business processes". |
| Request for definition – "cyber risk levels" (2.2.2.) | Clarification | Para. 12 of Section 2.2.2. requires the FMI to monitor connections among assets and cyber risk levels. Please provide clarification on what is meant by "cyber risk levels" in this context. |

| | | |
|---|---|---|
| Specific comment – Inventory of accounts (2.2.2.) | Clarification | Para. 7 of Section 2.2.2. expects the FMI to maintain an "exhaustive inventory of all individual an system accounts […] to know access rights to information assets".<br><br>We consider the accounts in scope to be user or system authorizations to the FMI's core systems. In case the CROE require a larger scope of accounts to be encompassed by the inventory, we seek clarification on the concrete scope of accounts to be included. In case third party service providers having access to selected information assets for the processing of their service shall be encompassed as well, we would like to express our opinion that in such case no individual accounts should be included in the inventory but rather the access on legal entity level (service provider). |
| Specific comment – ISMS Certification (2.3.2) | Amendment | Para. 6 of Section 2.3.2 states that "the FMI should seek certification of its ISMS, which is based on well-recognized international standards."<br><br>While aligned standards are beneficial (see earlier comment on 1.3.), certification of the ISMS can only be a necessary but not sufficient requirement. Thus, the guidance should clarify the necessary level of control effectiveness (including a specified scope of ISMS related processes, alignment with OpRisk processes and adequate coverage of core security processes) rather than simplifying this to a certification only. From experience, certifications (ISO 27k, SOC1/2/3, etc.) are creating their own focus, not consistent with cyber resilience requirements. Consequently, the guidance should require a "frequent review against accepted standards" instead of certification. |
| Specific comment – Background security checks (2.3.2.2.) | Amendment | Para. 58 of Section 2.3.2.2 requires the FMI to embed information security at "each stage of the employment life cycle" as well as during their "ongoing management". This shall be ensured, among others, through performing background security checks on employees and contractors.<br><br>The conduct of continuous or recurring background checks on employees and contractors is currently no common practice, as the potential benefits of such continuous checks are expected not to outweigh the costs associated. Rather background checks are being conducted prior to entering a contractual relationship.<br><br>We therefore suggest to amend the respective oversight expectation accordingly and provide clarification that background checks shall be conducted prior to entering into contractual agreements and when information has been obtained indicating the necessity to perform a recurring background check. |

| | | |
|---|---|---|
| Specific comment – Monitoring of activities (2.4.2.) | Amendment | Para. 2 of Section 2.4.2. expects the FMI to monitor activities and events in order to be able to detect abnormalities. As a FMI's ability to monitor activities and events is limited by existing laws and regulations, e.g. the approval of the workers council, we suggest to amend para. 2 accordingly to reflects such limitations:<br>„FMI should develop the appropriate capabilities, including the people, processes and technology, to monitor and detect anomalous activities and events, by setting appropriate criteria, parameters and triggers to enable alerts, *under due consideration of existing laws and council rules*." |
| Request for definition – "Staff" (2.4.2.) | Clarification | According to para. 7 of Section 2.4.2 FMIs shall "ensure that its staff are trained […]". We ask for clarification on the term "staff" used. |
| Specific comment – Monitoring of activities (2.4.2.) | Amendment | Para. 14 of Section 2.4.2. expects the FMI to "have processes in place to monitor activities which are not in line with its security policy and might lead to data theft or destruction.". As activities leading to integrity compromises might have severe impact on the FMI as well, we suggest to include those and amend para. 14 accordingly:<br>"The FMI should have processes in place to monitor activities which are not in line with its security policy and might lead to data theft, *integrity compromise* or destruction." |
| Specific comment – Comparison of network traffic (2.4.2.) | Clarification | According to para. 17 of Section 2.4.2. the FMI shall compare its network traffic continuously with the expected traffic, configuration baseline profile and data flows.<br>The demand for continuous comparison lacks the principle of proportionality, which should be included in order to enable also smaller FMIs to comply with such requirement. In general, the oversight expectations should be related to the risks the respective FMI is facing.<br>Moreover, we consider the proper implementation of continuous comparison to be reflected in appropriate governance arrangements including relevant suppliers and entities within the respective outsourcing chain. |

| | | |
|---|---|---|
| Specific comment – Intrusion Detection (2.4.2) | Deletion/ Amendment | Para. 19 suggests, "The FMI should develop intrusion detection capabilities to automatically detect and block the attacks in real time, including zero-day exploits. The intrusion detection capabilities should assist the FMI to proactively identify vulnerabilities and deficiencies in its protective measures".<br><br>We need to be aware that Intrusion Detection and Prevention (IDP) technology deployed already is intrinsically ill-fitted for detecting zero-days, since those systems only detect known threat vectors. Zero-days, by nature, exploit unknown vulnerabilities, typically invisible to IDP systems. Thus, we suggest either deletion of this statement or amending it for a control target instead of citing a specific technology stack and zero-day (representative for unknown threats): "The FMI should develop threat detection capabilities which can detect both known and unknown threats, with a proactive identification of vulnerabilities, state-of-the art threat detection and correlation between vulnerabilities and threats". |
| Specific comment – Intrusion Detection (2.4.2.) | Amendment | FMIs expected to reach an intermediate maturity level are required to develop "intrusion detection capabilities to automatically detect and block the attacks in real time" according to para. 19 of Section 2.4.2. Under consideration of the maturity level as well as in order to be able to block attacks in real time, we suggest to expect the FMI to detect threats rather than only intrusion. Hence, we suggest replacing "intrusion" with "threat" in the aforementioned paragraph. |
| Specific comment – Deception mechanisms (2.4.2.) | Amendment | Para. 20 suggest the FMI to implement deception mechanisms for detection.<br><br>As already outline above on Section 2.4.2, we are of the opinion, that no discrete technologies should be expected or suggested. Deception is considered being effective at present but could be rendered ineffective in due course if new adversary approaches proliferate. We therefore suggest to amend the oversight expectations by replacing "detection" by "technologies inhibiting lateral movement". |
| General comment – RTO (2.5.2.1.) | Clarification | Para. 4, 9 and 16 target timely recovery after a cyber incident has occurred.<br><br>We would like to point out, that timely recovery (under consideration of set recovery time objectives; RTO) is only effective and reasonable after the root cause of a cyber threat has been identified and isolated. Specifically, in case of integrity compromise of critical data, immediate recovery would be counterproductive. In the draft oversight expectations at hand, we do not see that such considerations have been taken into account appropriately. We therefore suggest to respectively integrate those and expect the prior identification and isolation of the root cause to become a mandatory prerequisite and effective starting point for the RTO. |

| | | |
|---|---|---|
| General comment – RTO (2.5.2.1.) | Clarification | According to para. 14 of Section 2.5.2.1. FMIs of an intermediate maturity level shall be able to resume critical operations within two hours.<br><br>A full root cause analysis necessary to secure ongoing normal course of business may require a substantial amount of time. As such, it would be more than useful to specify further the degree of recovery to be reached within the RTO following a cyber incident.<br><br>Under due consideration of the overarching objective to avoid major disruptions of the financial system following a cyber incident on critical operations, we consider the timely information of participants and other stakeholders such that substitution of service affected can be initiated, may be sufficient to archive a RTO of two hours. |
| General comment – RPO (2.5.2.2.) | Clarification | Following our comments on Section 2.5.2.1. among others, para. 20 and 24 of Section 2.5.2.2 aim at ensuring data integrity. We would like to point out, that ensuring data integrity parallel to timely recovery following a cyber incident (particularly with fast RTO) is not reasonably feasible.<br><br>We therefore ask for clarification to whether and if, to which extent, the validation of data integrity is required prior to recovery. |
| General comment – outsourcing of forensic services (2.5.2.4.) | Clarification | Section 2.5.2.4. outlines oversight expectations regarding forensic investigations. Forensic resources are not equally available to FMIs of different sizes, hence external services, used on a fully trusted basis, should be allowed. We therefore suggest to explicitly include that forensic services can be outsourced. Please provide clarification in case specific requirements (beyond general requirements on outsourcing) should be considered when outsourcing forensic activities in this context. |
| Specific comment – Reference (2.5.2.4.) | Clarification | Para. 47 of Section 2.5.2.4. requires that based on “1), 2) and 3)” a Forensic Readiness Policy shall be implemented. Please clarify to what “1), 2) and 3)” is referring to. |

| | | |
|---|---|---|
| Specific comment – Forensic investigation (2.5.2.4.) | Clarification | The group of people involved in the conduct of forensic investigations often needs to be limited on an absolute need-to-know bases.<br>Forensic investigations can be triggered by different events. Clarification is requested on the different treatment expected for on the one hand e.g. fraud and inside-driven cyber events, where the involvement of compliance, legal and executive management is required, and on the other hand IT or outside-driven cyber events, where usually a broader set of organizational units and functions, basically the entirety of crisis and incident management processes will be triggered. |
| Specific comment – TIBER-EU framework (2.6.1.) | Amendment | According to para. 31 of Section 2.6.1. FMIs shall use the TIBER-EU framework to conduct red-team exercises.<br>The TIBER-EU framework requires red-team exercises to be conducted by external parties. Conduct of red-team exercises should not be limited to external parties. In our view, the conduct of red-team exercises by internal parities should be acknowledged as being sufficient to meet the expectation, as long as the red-team exercise is conducted by an independent party. |
| Specific comment – Scope of testing programme (2.6.2.) | Amendment | Para. 1 of Section 2.6.2. requires that the FMI's testing programme covers "each component of the cyber resilience framework", which should be monitored, assessed and evaluated. Under consideration of para. 8 of Section 2.1.2.1., where it is stated that the cyber resilience framework shall incorporate requirements related to, among others, governance as well as learning and evolving, we suggest to amend the requirement to avoid misinterpretation that the testing programme also covers the governance framework as well as learning and evolving. We suggest to change the wording by deleting "each" in sentence 2 of para. 1 of Section 2.6.2. and replacing it by "core". |
| Request for definition – "independent parties" (2.6.2.) | Clarification | Para. 4 of Section 2.6.2. expects tests to be undertaken "by independent parties". Please provide clarification on what is to be considered independent within this context. |
| Specific comment Scenario analysis (2.6.2.) | Amendment | While para. 15 requires "extreme but plausible scenarios" to be simulated, para. 18 requires the consideration of "unconventional scenarios". We suggest aligning wording used and only refer to "extreme but plausible scenarios" or, alternatively, specify what is to be considered "unconventional scenarios". |

| | | |
|---|---|---|
| Specific comment – collaborative testing (2.6.2.) | Amendment | Para. 34 requires the FMI to regularly conduct tests in collaboration with (among others) peers. While we generally support a collaborative approach, the ECB should consider that the number of FMI expected to reach an advanced maturity level, particularly of one type (CCP, CSD, SSS, etc.) comparable in size and services offered, will be most probably very low. Moreover, the ECB should consider, that such an approach for advanced maturity levels, which will affect only selected FMIs, might foster convergence in testing, which will rather reduce FMIs ability to also consider unlikely threads.<br><br>We suggest to consider revising this expectation or providing clarification on the term "peer" used. |
| Specific comment – sharing of test results (2.6.2.) | Deletion | Para. 38 requires the FMI to share the test results with relevant stakeholders. We would like to point out that appropriate "reading" of test results requires specific knowledge of Cyber Resilience Frameworks in general as well as of FMIs in particular and is often only valuable if reference results are available to stakeholders. Sharing of test results with potentially unsophisticated stakeholders might result in misinterpretation of those. Moreover, oversight expectations with regard to (general) information sharing are specified under Section 2.7.2.2. and should be bundled there. We consider sharing of information as required under Section 2.7.2.2. on e.g. modus operandi of attackers as well as on threats, as sufficient and more purposeful to increase cyber resilience as well as awareness to cyber threats than general sharing of test results. Hence, we therefore suggest to delete para. 38 of Section 2.6.2. |
| Specific comment – External information (2.7.2.) | Amendment | Para. 4 lit. c of Section 2.7.2. requires the FMI to "analyse information security incidents experienced by other organisations". As the availability as well as quality of external information can hardly be influenced by the respective FMI, the oversight expectations should not mandatorily require the FMI to analyse such information, but rather limit such expectations to where respective external information is available. |
| Specific comment – Reporting of cyber threat (2.7.2.1.) | Clarification | Para. 10 of Section 2.7.2.1. expects the FMI to develop a Cyber Threat Risk Dashboard and Reports. We suggest to explicitly clarify that reporting on cyber threats can be integrated in existing IT-risk reporting, in order to provide information most efficiently and avoid duplication of existing reporting processes. |