4 June 2018

EUROPEAN CENTRAL BANK CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES

ECSDA CONSULTATION RESPONSE

The European Central Securities Depositories Association (ECSDA) represents 38 Central Securities Depositories (CSDs) across 35 European countries. As regulated financial market infrastructures, CSDs play a vital role in supporting safe and efficient securities transactions, both domestic and cross-border. If you have any questions on this paper, please contact Ms. Anna Kulik, Secretary General of ECSDA, at info@ecsda.eu or +32 2 230 99 01.

On 10 April 2018, the European Central Bank (ECB) launched a public consultation on the ECB's draft report with proposed Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures (FMIs). The CROE includes the ECB's expectations in terms of cyber resilience, based on existing global guidance. This paper constitutes ECSDA's response to the consultation, focusing on the perspective of European Central Securities Depositories (CSDs). The draft report forms an excellent basis for improving cyber resilience of FMIs. It also supports FMIs in the implementation and operationalisation of the existing global guidance, i.e. the "Cyber Guidance" issued by the CPMI and IOSCO in 2016 as a complement to the 2014 Principles for Financial Market Infrastructures.

We are appreciative of the ECB fostering the principle of proportionality and taking a reasonable approach which will contribute to meaningful discussions between FMIs and their overseers, as:

- The CROE correctly identifies that there should be a degree of flexibility when dealing with a heterogeneous group of FMIs. Even though a CSD is an FMI, there are substantial differences with other FMIs and amongst CSDs which justify a proportional approach.

- The CROE is to be considered a set of practices that can contribute to an FMI's compliance with the Guidance. We welcome the acknowledgement that the CROE is not put forward as a checklist of measures FMIs need to strictly comply with and that there is a graduation in the level of compliance to be reached.

- The CROE is meant to be used as a reference document which has been aligned with global and international standards and frameworks. Global CSDs are governed by multiple overseers and thus confronted with a regulatory fragmented landscape. The CROE will contribute to supervisory convergence as it can be used as a single reference document across multiple jurisdictions.

Nonetheless, we believe that a few issues require further consideration by the ECB before the CROE is published in its final form. In particular:

- The ECB's oversight is limited to payment systems and T2S. For 'other' FMIs like CSDs, the ECB refers to the National Competent Authorities (NCAs) to decide how they will need to apply the CROE and what is the maturity level they expect the FMI to reach. This could open the door to more regulatory fragmentation for CSDs and an unequal level playing field depending on the views local authorities take. We would like to encourage the ECB to ensure further alignment with ESMA, to avoid that each NCA takes its own view on this matter.

- We ask for greater alignment between the CROE and inherent risk assessment models, like the Cybersecurity Capability Maturity (C2M2) model. Concrete explanations are provided in the consultation's feedback table. However, we would like to avoid that CSDs become exposed to multiple and divergent expectations from the NCAs depending on whether they align with CROE and/or other inherent risk models.

- We have no doubt that Eurosystem will ensure that appropriate actions are taken to prevent a cyber-attack at the level of T2S. However, when speaking about CSDs, the CROE does not appear to consider the current situation of dependency of CSDs on the Eurosystem in terms of cyber security exposure and requirements. The Eurosystem (as T2 and T2S provider) is a key provider to the CSDs and thus there is an important dependence to ensure an appropriate level of CSD cyber resilience. Particularly when an attack occurs at the level of the Eurosystem and directly or indirectly impacting securities transactions, the response, responsibilities and consequences for CSDs need to be cleared. In addition, there are further ramifications on the CSDs liability in view of the T2S Framework Agreement.

- In our view it would be beneficial if CROE could clarify the expectations for regulated entities belonging to a group or being part of a corporation.

Detailed comments are provided in the consultation's feedback table. We remain at your disposal to provide any further information.

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.	Anna Kulik
	info@ecsda.eu	
	003222309901	
☐	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)	ECSDA	ISO code of the country of the originator	BE

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

Issue	Comment	Reasoning
1.4.1. Levels of maturity	amendment	The community of CSDs supports and welcomes international alignment of assessment methodologies to ensure a global level playing field and exchange of best practices. As example, in June 2015, the Federal Financial Institutions Examination Council (FFIEC) released the Cybersecurity Assessment Tool (Assessment) to help institutions of all sizes identify their risks, assess their cybersecurity preparedness, and help inform their risk management strategies. For more information, please visit the FFIEC's Cybersecurity Assessment Tool webpage at http://www.ffiec.gov/cyberassessmenttool.htm. The assessment tool was updated in May 2017. The CROE also considered the C2M2 model (as stated in CROE, page 6, section 1.2.). Although the levels of maturity defined in the CROE do not fully map with the FFIEC C2M2 assessment model. Global FMIs are subject to multiple oversight expectations. Smaller CSDs might have international participants having certain expectations of CSD compliance with the existing other guidelines. Hence, it would be helpful to use the same standard levels of maturity (e.g. of the C2M2 model). The model leaves more flexibility for individual supervisors and overseers to determine the appropriate level of maturity for the FMIs in their jurisdiction.
1.4 Requirements by type of FMI	Clarification	The ECB states "For other relevant regulatory, supervisory and oversight authorities that intend to use the CROE for other types of FMIs (e.g. CSDs, CCPs and TRs) under their responsibility, it is at the discretion and judgement of the authorities to determine what level of maturity they expect from the FMIs. "The C2M2 model provides authorities (or any other user) with a tool to determine the inherent risk of an FMI. It would be helpful if this inherent risk tool would also be part of the CROE. FMIs, for reference of the authority, and also in case a local authority does not choose to use the CROE tool, could use the tool individually without guidance.

2.1. Governance	Clarification	In our view it would be beneficial if CROE could clarify the expectations for regulated entities belonging to a group or being part of a corporation. For example, we would deem it appropriate for an entity which is part of a group to be able to implement a common group policy or framework, as long as (i) the steering document is meaningful for the given entity and its Supervisory Board, (ii) the Board of Directors has been sufficiently informed and (iii) a decision in that sense has been taken.
2.1. Governance expectations 2.1.2.1 – Cyber resilience strategy	amendment	The CROE states that: "The FMI should establish an internal, cross-disciplinary steering committee comprised of senior management and appropriate personnel from multiple business units to collectively develop a cyber resilience strategy and framework." The CPMI-IOSCO cyber guidance refers to the board guidance with appropriate distribution of responsibilities, culture, skills and accountability. The C2M2 statement (D1.G.OV.B1) for governance is "Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs." While these three statements broadly match, the additional level of detail included in the CROE is more confusing on the level of the committee accountable and responsible for the cyber resilience strategy. 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 CISO.
2.1.Governance expectations 2.1.2.1 – Cyber resilience strategy	amendment	Point 5 of the governance expectations refers to "The FMI's Board should approve the cyber resilience strategy, and should ensure that it is regularly reviewed and updated according to the FMI's threat landscape." We would suggest making it the first point in order to highlight the importance of the board involvement.

Governance expectations 2.1.2.1 – Cyber resilience framework	amendment	Point 11 refers to "The FMI's Board should endorse this cyber resilience framework, ensuring it is aligned with the FMI's formulated cyber resilience strategy, **and review and update it, at least annually,** to ensure that it remains relevant." A CSD's Cyber Resilience framework is a long-term strategic document and annual updates might be contradictory to this long-term perspective. Would be a more neutral phrasing: "The FMI's Board should endorse this cyber resilience framework, ensuring it is aligned with the FMI's formulated cyber resilience strategy, **and review and, *when needed,* update it~~, at least annually,~~** to ensure that it remains relevant."
Governance expectations 2.1.2.1 – Cyber resilience strategy and framework	clarification	Point 15 (on page 15) refers to a long-term objective maturity level. As cyber threats change constantly, we propose a more risk-based approach versus a maturity-based approach. A long-term objective for maturity is contra-intuitive as the maturity levels do not always match the risk of a certain weakness or emerging threat. Hence, a long-term objective is hard to establish and to obtain. Priority may need to be given to continuous improvement on critical risks, rather than an overall maturity increase, even on minor threats. We would therefore welcome a phrasing to incorporate the recognition of the fact that it is even more important to focus on critical risks than on an overall maturity (which is important as well).

Governance expectations 2.1.2.2. – Board and management responsibilities	amendment	Point 20 refers to a direct report to the board of the CISO. "The senior executive should [..] report directly to the Board." We note that CROE proposes very detailed requirements in terms of governance expectations which goes far beyond the CPMI-IOSCO Guidance and do not allow to accommodate different size and organizational structures of FMIs. As regard to the role of CISO we share the view that it is a key organizational role for cyber resilience, however FMI should retain the necessary flexibility to define its set-up according to its own organizational structure, although having a possibility to communicate directly with the Board. This should be without prejudice to the fact that the CISO has sufficient "authority, independence, resources and access to the board" as provided in CPSS-IOSCO Guidance (§§2.3.4). 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."
ANNEX 3 – Guidance to the senior executive	Deletion	As per the comment above we believe that ANNEX 3 should be revised in order to cater for different size and organisational model of FMIs (such as FMIs that are part of a group structure). 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 proper information flow and access to the Board shall be allowed under the CROE. Therefore, we suggest deleting point 2(b) and clarify the term "in house" allowing for a group-wide CISO, if appropriate, in point 4 of the Annex.

2.3 Protection Network and infrastructure management, Points 11 to 22	Clarification	In point 2.3.1, the CROE states that controls should be designed according to the threat landscape and "consistent with its risk tolerance". However, in points 11 to 22 of 2.3.2.1.2, controls are listed without consideration of the risk-based approach. A statement that a risk-based control approach is applicable to these points would be appreciated.
2.3 Protection Point 42	Clarification	Point 42 refers to: "The FMI should use an Attribute-Based Access Control (ABAC) paradigm that allow it to, contextually and dynamically, manage the access to its IT environment." This does not appear to have been included in the CPMI-IOSCO guidance. Hence, some context to this requirement would be appreciated.
2.3 Protection Point 58	Clarification	Point 58 refers to "the FMI should carry out background security checks on all candidates". In some countries such a background check is forbidden or limited to certain tasks. We would therefore welcome either a more neutral wording or clarification on a solution in these cases.

2.5.2 Response and recovery Point 14 (on two hour recovery)	clarification	Point 14 states that : "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 exercise judgment 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. " We welcome the clarification that the FMI should exercise judgment in effecting resumption. This is crucial that in case of cyber-attacks which could generate a systemic effect, even if the triggering event affects one entity only. 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 undermines the integrity of data, 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 operation is based on 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 appropriate)** 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." In addition, with reference to the requirement to complete settlement by the end of the day, we would like to recall ECB attention to the fact that in case of cyber-attacks having systemic impact, the decision to resume settlement operation shall be the result of a joint assessment performed by the FMI, participants and competent authorities jointly.

2.5.2 Response and recovery Point 14 (on two hour recovery)	Clarification	Point 14 states that: "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 exercise judgment 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." In addition to our earlier comment on that point, The CPMI-IOSCO guidance states in addition to the above provisions : "While FMIs should plan to safely resume critical operations within two hours of a disruption, **they should also plan for scenarios in which this objective is not achieved**. FMIs should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of the FMI, facilitate the processing of critical transactions, for example, while remediation efforts continue. FMIs should also plan for situations where critical people, processes or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible, safe and practicable, to manual processing if automated systems are unavailable." We do not see this reflected in the CROE guidance. Some related pieces are found in other points of the CROE that could constitute the CPMI-IOSCO guidance. We would also appreciate a clarification on how to achieve the second point of the CPMI-IOSCO guidance when people and resources are unavailable for significant periods.
2.5.2.2 Response and Recovery – data integrity paragraph 25	Clarification	We would welcome clarification on the meaning of "independent reconciliation of participant position".

2.6.2 Testing-Expectations Point 42	clarification	Point 42 states that: "In addition to periodic independent, external red-team exercises, the FMI should develop an internal red-team capability, with the appropriate methodologies, sophisticated tools and appropriately skilled personnel." For smaller FMIs, this would not be feasible as the investment to have a team of red-team testers is too substantial. However, even smaller FMIs can be considered systemically critical and thus be required to have this capability.