EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

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

Name of the originator (i.e. name of the company or association)	INSTITUTE OF INTERNATIONAL FINANCE	ISO code of the country of the originator	US

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

Issue	Comment	Reasoning
Introduction (Section 1.2 Purpose): Requires immediate compliance with the guidelines once it is published	Amendment	In terms of the implementation timeline, there could be practical issues concerning the availability of qualified staff on the overseers' side to assess the FMIs under their responsibility and determine their cyber resilience maturity levels. Hence ECB may consider adopting a phased-in approach to implementation (assessing first the most critical FMI's) as opposed to the implementation timeline being immediate.
Introduction (Section 1.2 Purpose): it states that overseers must simultaneously develop an oversight approach to assess their FMIs against the Guidance.	Clarification	Overseers should commit to develop approaches in a coordinated manner to avoid further regulatory fragmentation which could exacerbate operational risks to firms, and therefore inadvertently lead to more risk and financial instability in the ecosystem.
Introduction (Section 1.3 Addressees): mentions "principles", "guidance" and "laws and regulations"	Clarification	Strong clarification is needed to stress the importance of harmonized and coordinated guidance, frameworks and regulations, and to highlight that fragmentation could inadvertently lead to increased operational risk and possibly financial instability.

Introduction (Section 1.4.2): The Guidance establishes which FMI's should maintain at least a Baseline or an Intermediate level of maturity.	Amendment	Although the concept of maturity level is well understood (but difficult to measure) and makes sense for setting expectations about the cyber-resilience of FMI's, the concrete level of maturity at which each individual FMI is or should be, must be the consequence of an in-depth dialogue between them and the overseers. Each FMI's particular set of circumstances, their individual strengths or weaknesses or their overall cyber-resilience posture, should all inform the final classification, but in a much more flexible and dynamic way. However, overseers should share common guidance on the criteria to follow when deciding on that classification**.**
Introduction (Section 1. 3 - Addresses): It is important for FMIs to take on an active role in outreach to their participants and other relevant stakeholders to promote understanding and support of cyber resilience objectives and their implementation	Clarification	It is not clear the real extension of the network of stakeholders to consider and the criteria, conditions and constraints to evaluate for their implementation of CROE.
Governance (Section 2.1.2.1 paragraph 2, f): This paragraph refers to cyber resilience strategy design	Amendment	The steering committee should specify that the strategy encompasses objectives to achieve in ordinary context, and objectives (or minimum required service level) to achieve in case of occurrence of extraordinary events.

Governance (Section 2.1.2.2 paragraph 13): States that the FMI should use relevant metrics and maturity models to assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework through independent compliance programmes and audits carried out by qualified individuals, on a regular basis	Clarification	There should be coordination on metrics and maturity models in order for the information on relative security to be useful.
Governance (Section 2.1.2.2 paragraphs 19 & 22): Those paragraphs contain references to the Board expertise in cyber-risk	Clarification	The drafting of those two paragraphs would benefit if the document made clear that the Board should have access to cybersecurity expertise. For the IIF members it is important that Boards have access to internal, external, and independent experts to ensure that they adequately understand cybersecurity risks, but the composition of a Board should be driven not by a specific skill set but by the overall experience of each member and the combination of experience across the board. As such, the Board should consist of directors with a diverse set of experiences and qualifications, including cybersecurity.
Governance (Section 2.1.2.2 paragraph 27): Senior management should ensure that situational awareness materials are made available to employees when prompted by highly visible cyber incidents or by regulatory alerts.	Amendment	We recommend that instead of making situational awareness material available to all employees it should be modified to say relevant employees.
Governance (Section 2.1.2.2 paragraph 36): The Guidance requires a draft of a specific Cyber Code of Conduct	Amendment	The IIF member firms have a Code of Conduct that covers the appropriate use of its systems. It is recommended that the ECB consider clarifying that these statements are not required to be placed in a separate document.

Identification (Section 2.2 Paragraph 8): Requires an AIM	Clarification	The identification mentioned in this paragraph has to be centralized. However the ECB should clarify how to consider the organizational structure of a worldwide Group with different regulations across various geographies and its challenges for data sharing.
Identification (Section 2.2 Paragraph 14): The guidance establish that the FMI should identify emerging risks in real time, and use automated feeds from above (i.e. AIM and IAM), in order to continuously update its risk assessments and take the necessary mitigating actions, in a timely manner and in line with the FMI's risk tolerance. This statement should be amended with: …the cyber risk assessment program should be documented and periodically evaluated against shifts in the FMIs threat landscape to ensure that the risks to these emerging threats are well understood.	Amendment	A risk assessment is a point in time review of an application, infrastructure or process to identify gaps in the minimum control standards set forth by the organization. Therefore, the risk assessment program is not normally updated in a real-time manner. The program may be updated when there are updates to minimum control standards, integration of new technology, new business products, shifts in the threat landscape, etc. but these processes are not normally updated based on continuous, automated feeds. It is recommended that the ECB considers how firms evaluate and make changes to their risk assessment program.
Protection (Section 2.3.2.1.1 paragraph 5) This paragraph refers to the adoption of a redundant framework of security controls	Amendment	The redundancy of the controls could be adopted with a risk based approach. The objective to achieve this should focus not on the redundancy of controls, but on the identification of potential complex events of risk that can be generated by the increase of interconnections and dependencies of internal and external factors, by the evolution of processes, system and people skills. These events should be accurately assessed and evaluated in terms of controls already in place and controls to be implemented taking into account that costs for controls should not exceed the benefit that could be obtained by their implementation and real execution.

Protection (Section 2.3.2, paragraph 6): The guidance establish that the FMI should seek certification of its ISMS, which is based on well-recognized international standards.	Amendment	There is a need for more clarity on this statement. An FMI can have an independent audit or review of the ISMS but a certification as stated implies that the organization must seek something outside of an independent audit/review of its systems (e.g., SOC1/SOC2) to certify compliance to a specific standard (e.g., ISO 27001, CSA STARS). Firms may use a combination of different standards to develop their cyber risk and control structure. Requiring certification may force FMIs to alter the current protections that they have in place to manage the risks to their systems in order to meet a certification requirement, and shift valuable resources from risk management objectives to certification initiatives that may not improve the security of the FMI. The IIF members recommend that the ECB considers the use of the word ***review*** instead of ***certification***.
Protection (Section 2.3.2.1.2 paragraph 11): The FMI should establish a secure boundary that protects its network infrastructure, using network perimeter defence tools such as router, firewall, IPS/IDS, proxies, VPN, DMZ, etc. The boundary should identify trusted and untrusted zones according to the risk profile and criticality of assets contained within each zone, and appropriate access requirements should be implemented within and between each security zone according to the principle of least privilege.	Amendment	We suggest that this requirement should be redrafted to capture a principal based approach to state that, "The FMI should implement network segmentation in their organization, which meets the principle of least privilege."

Protection (Section 2.3.2.1.2 paragraph 17): The FMI should activate and configure local firewalls on workstations and endpoint systems, including devices used for accessing the FMI network remotely to block by default administration ports except from explicitly identified devices (e.g. administration).	Amendment	We recommend that ECB should modify this statement to read, "The FMI should ensure that default administrative access to systems is restricted. Only authorized individuals from authorized devices should be allowed to carry out administrative tasks".

Protection (Section 2.3.2, paragraph 19): The FMI should implement controls that prevent non-controlled devices to connect to its internal network (e.g. personal devices, rogue access point, etc.) and endpoints (e.g. removable media), from inside the premises or outside (e.g. remote connections). The FMI's infrastructure should be regularly scanned to detect rogue devices and access points.	Amendment	FMIs employ guest wired and wireless access points that allow for visitors (clients), regulators and other third-party audit organizations to access resources on their home networks. This statement, as written, may have the unintended consequence of preventing the use of these technology solutions. While these endpoints are not controlled by the FMI, the FMI should institute controls to limit the access of these devices to its production computing environment. Therefore, it is recommended that the ECB consider revising this statement to reference that the FMI control these points. As an example, this statement may read: *The FMI should implement controls that manage or prevent non-controlled devices to connect to its internal network from inside or outside of the premises to ensure that activities in these zones is logged and monitored for inappropriate use or attempts to access business systems. The FMIs infrastructure should be regularly scanned to detect rogue devices and access points*.
Protection (Section 2.3.2, paragraph 36): The FMI should develop appropriate controls (e.g. end-to-end encryption, authentication and access control) to protect data at rest, in use and in transit. The controls should be commensurate to the criticality and the sensitivity of the data held, used or being transmitted, as per the risk assessment conducted in Identification.		The encryption of all the information within the network may significantly decrease the ability for detection within the organization. In certain countries, the encryption of the data is not allowed or severely controlled by government. Other countries do not allow deciphering of communication on the fly for detection purpose. A balanced, pragmatic approach is recommended considering the cost/benefit analysis (or risk based approach).

Protection (Section 2.3.2, paragraph 38): The FMI should implement technical controls that trigger automated notification to appropriate personnel whenever user access permissions change. Controls should be in place to prevent unauthorized escalation of user privileges.	Deletion	The implementation of this control could ultimately create hundreds, if not thousands, of alerts and ultimately lead to an ineffective control due to the volume of alerts received by an analyst. The processes of the creation of new users, user transfers, and leavers would all generate alerts which would require time consuming and costly analysis without a corresponding benefit in terms of improving the security of an FMI. Policies and procedures should be in place, but the methodology and tools used to carry out the control should not be specified.
Protection (Section 2.3.2, paragraph 58): The guidance requires recurrent background checks on all their personnel.	Amendment	While most firms conduct those checks upon entrance into their firms, the practice of recurrent background checks on this same population is not a common practice and could result in significant costs for little or no benefit. It may be more appropriate to limit the completion of these checks on employees in sensitive positions, especially as a Baseline control.
Protection (Section 2.3.2.3, paragraph 71): The FMI's third-party risk assessment should be carried out regularly, taking into account the evolution of its threat landscape. The FMI should ensure that the provisions of outsourced services are accorded the same level of cyber resilience as if they were provided by the FMI itself.	Clarification	This is a very valid and important requirement. However, we recommend that the level of cyber resilience requirement by third party be determined by the type of service outsourced following a risk based approach.

Detection (Section 2.4.2, paragraph 19): 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	Deletion	The definition of a zero-day exploit is that these exploits take advantage of unknown or unpublished vulnerabilities. Therefore, when an exploit is launched under these circumstances, it is difficult, if not impossible, to detect or protect from these exploits. In addition, in order to provide protection for these exploits, it is often necessary for the vendor to develop a software patch or version upgrade to address these vulnerabilities. Therefore, zero-day exploits should not be included in that paragraph as a requirement.
Response & Recovery (Section 2.5.2, paragraph 14): Here the Guidance establish a two-hour resumption of critical operations.	Amendment	Given the unique characteristics of a cyber-attack, the ability to recover business operations and ensure that the environment is safe to reconnect to the financial ecosystem within a two-hour time period may increase the contagion risk of a significant cyber-attack. That is because in such an event, at a minimum, the FMI would need to locate the malware/virus that has infiltrated the system, reverse engineer the malware/virus to determine how the virus works and is promulgated, determine how to effectively remove the virus from the system and develop sufficient evidence to provide assurance to the financial services sector that the malware has been removed or contained. Instead of a hard rule, it is safer and more efficient to sustain a good governance model that addresses cyber disruptions scenarios and concerns as well as how to respond and recover from such attacks. Cyber threats are constantly evolving and include a diverse set of potential actors. Hard rules, particularly in this regard, could inadvertently hinder a company's ability to appropriately respond to, and protect other financial market participants from, such threats.

Response & Recovery (Section 2.5.2, paragraph 42): The FMI should develop a range of cyber incident scenarios	Clarification	With constantly evolving threats, there should be more focus on risk and vulnerabilities, rather than focusing on identifying the right threat scenarios.
Response & Recovery (Section 2.5.2.3.2, paragraph 43): The FMI should develop mechanisms to provide instantaneous notification of cyber incidents to its senior management, relevant employees and relevant stakeholders (including oversight and regulatory authorities) through multiple communication channels with tracking and verification of receipt. Such mechanisms should be based on predefined criteria and informed by scenario-based planning and analysis, as well as prior experience.	Clarification	We request the ECB to clarify on the need to provide notification from multiple channels, as this increases the attack surface area and impinges on the time of stakeholders and senior management.
Response & Recovery (Section 2.5.2, paragraph 52): The FMI should ensure that staff involved in handling evidences have the appropriate degree of competence..."	Amendment	We would suggest adding "trust" in addition to competence.

Testing (Section 2.6.1, paragraph 31&32): The FMI should use the TIBER-EU framework to conduct the red-teaming exercises. The FMI should outsource the conduct of red-teaming exercises to external, third-party providers. Simultaneously, the FMI should build its internal processes and capabilities to undertake the externally outsourced exercise (e.g. establishing an internal White Team, developing incident escalation procedures, following appropriate methodologies and establishing robust risk management controls), as set out in the TIBER-EU framework.	Clarification	The TIBER-EU program requires that external parties conduct the red-teaming exercises. We believe that, on a case by case basis, and with the approval and oversight of the regulator during testing, FMIs with the appropriate capability should be allowed to lead their own red-team in order to better minimize operational risks and increase data security as data may be contained within the FMI itself. This is consistent with GFMA's "Framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry" and the CPMI-IOSCO guidance, Guidance on Cyber Resilience for Financial Market Infrastructures, which reads, '…A red team may consist of an FMI's own employees and/or outside experts, who are in either case independent of the function being tested.' We recommend that ECB should modify this statement to allow for the use of in-house RED Teams. FMI's have established independent teams which provide these in-house services to the firms on a regular basis and we strongly urge that ECB allows the use of such teams for testing.
Testing (Section 2.6.1, paragraph 38): The FMI should share the test results with relevant stakeholders to boost the cyber resilience of its ecosystem and the financial sector as a whole, as far as possible and under specific information sharing arrangements.	Amendment	In general, Firms do not provide testing results to their clients or peers. While they will inform and provide evidence that testing has been completed, the testing results may contain proprietary and/or sensitive information regarding the organization's vulnerabilities and might even create new risks. While we promote the FMIs working together to build a resilient ecosystem, the detailed knowledge of individual FMIs vulnerabilities is not required to capture this goal. Additionally, we recommend that this statement should be modified to clarify that those specific information sharing arrangements should also be subject to any member state requirements.

Situational Awareness (Section 2.7): States that the FMI should belong or subscribe to a threat and vulnerability information sharing source and/or information sharing analysis centre…	Amendment	While this can be useful, there is often the case of sharing "too much information" whereby the haystack gets bigger and the needle becomes harder to find. It is more important to promote deeper operational collaboration, i.e., conducting exercises and sharing tactics and techniques.
Situational Awareness (Section 2.7) and Learning and Evolving (Section 2.8)	Clarification	Consider moving these Sections under the Section on Governance to make them more coherent.

ANNEX 3 – GUIDANCE ON THE SENIOR EXECUTIVE "2. The Senior Executive or CISO function has in particular the following tasks: a. Supporting senior management and the Board when defining and updating the cyber resilience policies, and advising on all cyber resilience issues; this includes helping to resolve conflicting goals (e.g. cost-efficiency versus cyber resilience);… i. Investigating cyber incidents and reporting these to the senior management and the Board;… l. Reporting to senior management and the Board regularly, at least quarterly, and on an ad hoc basis on the status of cyber resilience issues. This status report includes, for example, an evaluation of the cyber resilience situation compared with the last report, information about cyber resilience projects, cyber incidents and the results of penetration and red-team tests. 3. In terms of organization and processes, the Senior Executive or CISO must be independent to avoid any potential conflicts of interest. Therefore, the following measures, in particular, are expected to be applied: a. Organizational set-up to ensure the Senior Executive or CISO can act independently from the IT/operations department and be able to report to senior management and the Board directly and at any time; also ensuring that the Senior Executive or CISO is not involved in internal audit activities"	Clarification	While we fully support the need for the CISO to report to the Board on a quarterly basis as a minimum, there needs to be further clarity around the expectation of independence of the CISO: • Usually the CISO is aligned with the Operations & Technology department so whilst there may not be a direct management line to the IT/operations department, there may not be a sufficient degree of independence. Clarity is needed here on what would suffice as sufficient independence. • The concept of "independence" usually comes from the second and third lines of defense, so there should be more clarity and guidance on the roles of each of those 3 lines of defense.