
EUROPEAN CENTRAL BANK
EUROSYSTEM

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

Contact details (will not be published)	Ms.	Nandini Sukumar
	nsukumar@world-exchanges.org	
	+44 207 151 4150	
☐	The comments provided should NOT be published	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)	WORLD FEDERATION OF EXCHANGES	ISO code of the country of the originator	GBR

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

Issue	Comment	Reasoning
2.1.2.1. Cyber resilience strategy and framework	Amendment	The WFE agrees that strategy is a critical area of focus for FMI cyber security. However, if the implication is that "strategy" and "framework" are or should be specific and separate products then there is a risk of being unhelpfully prescriptive, potentially promoting a "tick-box" mentality. The different scales, business focuses and cultures within each FMI need to be recognised, **and flexibility afforded to allow individual institutions to meet these needs via different documentation methods**. For example, some FMIs will have a single "Strategy" document that captures everything intended in a strategy *and* framework. Others will have interlinked procedural documents that incorporate many framework elements while moving overarching strategic elements to mission and vision statements. Still others will have direct Board engagement in developing tactical policies. Whilst we applaud the positive intentions of the CROE, we consider they can be better met by noting that a **high-level strategy should be developed, documented, and informed, and that policies and procedures established to execute that strategy should be documented and maintained.** Further, it is recommended that any mentions of a "strategy" or "framework" be consolidated into the single term "Strategy".

2.1.2.2. Role of the board and senior management	Amendment	In an increasingly electronic world, operational resilience – and within that cyber resilience – has naturally become a key area of focus and risk for exchange and CCP Boards and Chief Executives, many of whom speak publicly of the risks and their concerns around the issues. Chief Information Security Officers (CISOs) are regularly and as a matter of course asked to **brief their Boards on recent developments and of the level of preparedness at the individual firm level. This has now become part of the "business as usual" within individual institutions.** *Bullet point 36* mandates that FMIs should adopt a formal Cyber Code of Conduct. While we agree with the intentions here, **CROE shouldn't be explicit in calling out a specific document**, but there should be a note to call out cyber in the overall FMI's Code of Conduct. *Bullet point 46* mandates that cyber resilience awareness information is provided to its participants regularly. While the objective here is clear, **we feel that in practical terms this requirement is more aligned with retail sector, and shouldn't be imposed at FMIs.**

2.2. Identification	Amendment	The WFE notes that the "Situational Awareness" and "Threat Intelligence" – as described in section 2.7 – may be better considered in the "Identification" phase of security programme management. In merging content (and, as it happens, more tightly aligning with the US National Institute of Standards and Technology (NIST) Cybersecurity Framework), this shifts the focus of the identification process, from a *"keys to the castle"* approach of asset discovery and classification, to a *"what are they after?"* approach of identifying threat actors and potential vectors of attack. This is particularly important for FMIs. While much of today's industry guidance around cybersecurity is informed by events in the retail space (e.g. theft and exfiltration of personal and payment card data), other industries are right to **focus on availability and avoiding tampering or disruption**. For FMIs, this threat is much more relevant and the choice of specific asset to target is less important than disrupting any of many interconnected links that would result in outage or instability. To that end, **identification efforts should be focussed on identifying threat actors and categories, tools, and methods, so defences may be properly positioned and tested.** WFE members agree on the importance of considering the risks presented by the wider ecosystem, and consequently WFE's GLEX Cyber Group regularly discusses industry risks with each other at the CISO level and participates in industry-wide testing events. However, we caution that, since FMIs operate in an ecosystem with multiple other (FMI and non-FMI) actors, there is **a finite amount any single organisation can achieve outside its own system**. We therefore **support efforts by, and encourage, regulators to foster cooperation and support coordination by ensuring there are common standards**.

2.3.2. Protection	Amendment	FMIs agree with the need for strong and robust controls that are proportionate to, and consistent with, the FMI's risk appetite and role in the system. Sitting as they do at the junction of finance and the real economy, FMIs are aware of their systemic significance and as such invest time, resource and management attention in protection measures, including security controls, systems and processes. These processes continue to evolve along with the development of the markets. Within WFE GLEX members, the majority of the annual cyber budget is spent on protection measures. In a joint IOSCO-WFE member survey, 89% of respondents said cyber-crime can be considered a potential systemic risk, demonstrating the heightened need for protection.. However, we caution that not all FMIs are at the same stage of development and so risk tolerance, threat landscape and systemic roles can legitimately vary. As such, **we advocate that regulators, whilst rightly fostering a focus on protection, should remain sensitive to the fact that being overly prescriptive, or offering a one-size-fits-all approach, will not likely be successful.** Moreover, we would note the following: • FMI/regulatory examination **should focus on more than just encryption, patch management and system hardening**. Other controls generally also important: ○ **Access Control**: Documented, repeatable and audited processes should govern the process; ○ **Email Security**: Detective and preventative controls around inbound e-mail to mitigate risks of phishing and malware attacks. Known malicious sending infrastructure and attachment types must be blocked. ○ **Intrusion Detection and Visibility**: Networks used for critical functions - and likely to be employed in attacks - should have appropriate instrumentation and be monitored for suspicious activity and abuse; ○ **Internet Egress**: Content filtering should be in place to identify malicious web sites and block access from employee and data centre systems; ○ **Web Application Security**: For Internet-based connectivity, network-based systems independent from web servers should have visibility into traffic and the ability to identify & block malicious activity; ○ **Network Segmentation**: A default-deny philosophy should be enacted via firewalls and access control devices that prohibit unnecessary communication among systems; and ○ **Remote Access**: Internet-based remote access for employees should require multifactor authentication to nullify the value of credential capture.

2.3.2. Protection	Amendment	As previously indicated in our comments to section 2.2 above, whilst we note the interconnectedness risk and support a framework that seeks to build in protections from external third-party risks, **it would be unreasonable to expect an individual FMI to be able to wholly ensure its service providers meet the same level of cyber resilience as the FMI itself**. A more realistic approach to vendor and partner risk would be to segment and minimise access outright and monitor the residual vectors of access closely. Analysis of the security risk must take into account IT vulnerabilities not in isolation but within the context of business process. **The focus should be on controls that mitigate, including where appropriate treating external connections similarly to internet-based connectivity, terminating them outside the network perimeter, only allowing specific required and approved protocols and sources, and monitoring the resulting traffic with behavioural analytic tools.**
2.3.2.2. People management	Amendment	Analytics – particularly behavioural – are rightly emphasised here. The practical "insider threats" in the context of the CROE are those that result in destruction or destabilisation. As such, we consider that **security analytics would be better served by focussing on behavioural monitoring, determining baseline activity patterns with regard to systems and data accessed, and alerting as to any deviation from those patterns**. Additionally, more focus should be placed on mitigating the threat of internal attacks given bad actors from the outside can pretend to be internal users.
2.4. Detection	Amendment	Detection remains a key frontier for FMIs in the battle to contain cyber threats. The WFE acknowledges the need for strong controls and standards, and further supports the ECB's perspective that these controls and standards should be proportionate and consistent to the FMI's relative size, systemic importance, risk tolerance and specific needs.

2.5.2. Response and recovery	Amendment	FMIs acknowledge the responsibilities related to their role in supporting financial stability – including their ability to settle obligations when they are due. The focus of all FMIs' response and recovery strategy are to ensure that critical systems resume full operation as soon as possible and without compromising the orderliness of the market. Whilst working towards a swift resumption, it is however important to note that conditions will vary from incident to incident and from FMI to FMI. Within this, we respectfully note that FMIs are already incentivised to return to full and orderly operation as soon as possible for business and reputational reasons. In particular we note the following: • Incident response planning: The WFE supports the CROE's approach on incident response planning. **FMIs should thoroughly investigate any incident, even while taking immediate action to contain the problem as a standard course of action,** feeding back any "lessons learned" via industry groups such as the GLEX, where possible and appropriate. The industry also **backs stringent efforts on contingency planning and preparation** including consulting with stakeholders before establishing final plans. • Incident response: We consider the general premise of operational impairment and recovery are well-addressed in existing guidance and regulation, where recovery time objectives (RTOs) are appropriately and adequately considered. For the purpose of cybersecurity-specific guidance, however, **the notion of resumption within two hours is inappropriate.** We advocate that **RTOs should be left where it already exists in general and operational guidance and are omitted from cyber-specific materials.** • Design elements: Different businesses will have different applications of integrity checking and re-establishment. For some businesses and scenarios, recording participant intent and replaying it will be appropriate. For many others, however, the only realistic path is to: establish a point of loss of reliability; to invalidate transactions submitted after that point; and to return to a previous checkpoint to resume processing. As such, **there needs to be sufficient flexibility to allow each FMI to determine what is appropriate, not only for their business but for the specific scenario and impacts they face.** Further, in many cases it is the participants of the FMI that are the only entities properly positioned to conduct reconciliation activity, and this is often a real and regular part of daily processing in safeguarding against (non-cyber) operational error. **Allowing participants to drive and inform reconciliation requirements directly is self-policing and successful already.** Tasking the FMIs with "independent reconciliation" is therefore prescriptive, unnecessary and potentially ineffective. • Cybersecurity drills: Time matters when it comes to a cyber-attack. **One of the ways to improve a company's reaction time is by implementing cybersecurity drills**. Emergency fire drills are commonplace in working environments, and the nature of cyber-attacks requires the same approach.

2.6. Testing	Amendment	"Testing" is the only outlier in the set of terms "Testing", "Situational Awareness", and "Learning & Evolving". **Since "Testing" is applicable to all of the NIST categories, we suggest subsuming those activities into the existing categories where they most appropriately fit.** The emphasis on information sharing, collaboration, and exercise is appropriate. In practice, industry groups are already active and the appropriate duty for most FMIs is to identify and participate in these activities.
2.7. Situational Awareness	Amendment	We consider that the last two items ("Situational Awareness" and "Learning & Evolving") can be incorporated into NIST categories – namely "Identification" – and in the process stress the flexibility of the CSF and use the CROE as a practical example of adapting the cybersecurity framework to an area of focus.
2.8. Learning and Evolving	Amendment	We consider that the last two items ("Situational Awareness" and "Learning & Evolving") can be incorporated into NIST categories – namely "Identification" – and in the process stress the flexibility of the CSF and use the CROE as a practical example of adapting the cybersecurity framework to an area of focus.

Additional Comments	**We caution against being overly prescriptive** in the following instances: **2.1.2.2. Role of the board and senior management:** • *Bullet point 30* talks about the need for adoption of recognized well-known skills frameworks. While we fully agree with the need for ensuring the right cyber talent is identified, being prescriptive on the adoption of a specific framework will be counterproductive when this is implemented and likely unsuccessful. **2.2. Identification:** • *Bullet points 8 and 9* are overly prescriptive in mandating the tools that need to be used. It is more productive and likely to be successful if specific objectives are mandated rather than prescribing specific tools. • *Bullet point 15* is again overly prescriptive. In order to achieve what is being asked in this section, it requires that all members of the ecosystem start scanning each other for vulnerabilities. This is not practical. It's better to remove this point and rely on identification of threats that key participants in the FMI's ecosystem have using threat intelligence. **2.3.2. Protection:** • *Bullet point 6* shouldn't be prescriptive in listing certain standards. • *Bullet point 29* mandates the implementation of deception capabilities. This is overly prescriptive and could be counter-productive for some FMIs. The message here should be that FMI should seek to continuously explore new technologies (such as deception), which in some scenarios could be useful in enhancing defensive posture of the FMI. • *Bullet point 35* is overly prescriptive and could be counterproductive, especially in cases when FMIs are exploring new approaches to addressing the issue of "too many passwords to remember for users" based on recent password guidances (such as NIST Special Publication 800-63B) which advocate longer passwords and use of passphrases with longer renewal periods. • *Bullet point 45* mandates the use of ABAC. This is too prescriptive and should be removed. **2.4. Detection:** • *Bullet point 20* mandates the implementation of deception capabilities. This is overly prescriptive and could be counter-productive for some FMIs. The message here should be that FMI should seek to continuously explore new technologies (such as deception), which in some scenarios could be useful in enhancing defensive posture of the FMI. **2.5.2. Response and recovery:** • *Bullet point 47* about Forensic Readiness Policy approved by the Board is too prescriptive and should be removed.

Additional Comments	While information technology may lend itself to other kinds of defences – we advocate not trying to maintain a supposedly exhaustive list of mandated measures, instead focusing on desirable outcomes, allowing the toolkit to develop and to be deployed selectively by each distinct infrastructure as circumstances and experience render most appropriate. Deflection strategies are a current example of a potentially valuable component of that toolkit that is emerging at the initiative of industry and that, like any other, has to be fully evaluated to determine what role it may play, in its own right and relative to other techniques, given the ever-evolving nature of cyber-threats. As such, **we consider it generally good practice for FMIs to place emphasis on constant re-evaluation and bottom-up growth**, rather than a periodically updated list of top-down, supervisor-approved techniques. As previously noted, **we caution against being prescriptive, and therefore advocate that specific defensive techniques be considered by FMIs' in their cyber strategies on their merits on a case-by-case basis, situation by situation**, to ensure sufficient flexibility to meet the individual needs of FMIs, the markets they service, and the challenges/threats they face. Whilst PFMI Principle 23 (Transparency - Disclosure of rules, key procedures, and market data) is not referenced as a key PFMI informing the CROE, the WFE would nevertheless like to raise an important issue relating to that particular PFMI and its read-across to cyber-related matters. PFMI 23 notes that "All relevant rules and key processes shall be publicly disclosed…" to enable participants to have an accurate understanding of the risks, fees and other material costs incurred by participating in the FMI. Here, with regard to cyber-resilience, we respectfully suggest that transparency for transparency's sake is not always a desirable outcome and may not achieve the wider PFMI public policy objectives "…to enhance safety and efficiency in payment, clearing, settlement and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability". Whilst acknowledging the benefits of transparency generally, **any requirement to publicly disclose details on cyber resilience could be potentially detrimental to the objective and must be conducted in a carefully considered manner** to ensure disclosure of such information doesn't better equip potential attackers and increase cyber resilience related risk.