EBA CLEARING

Classification: Public
December 2022

EBA CLEARING's response to the FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting[1]

EBA CLEARING welcomes the FSB's objective to achieve convergence in cyber incident reporting. The proliferation of cyber incident reporting requirements, imposed by financial and other authorities, has created a fragmented regulatory landscape in which financial institutions and financial market infrastructures (FMI) are required to report the same cyber incident to multiple authorities, but in different formats and under different deadlines. EBA CLEARING appreciates the FSB's efforts to address this issue and respectfully submits the following observations in response to some of the questions in the FSB's Consultative Document.

Challenges to achieving greater convergence in CIR (Section 2)

Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?

EBA CLEARING, in its practice and in light of its regulatory obligations, distinguishes between cyber incident reporting, and cyber resilience.

EBA CLEARING would encourage the FSB to distinguish clearly between: (1) cyber incident reporting – i.e. a legislative requirement to report to a regulatory authority a cyber incident that meets certain criteria– and (2) matters that contribute to or enhance the cyber resilience of an organisation. In EBA CLEARING's view, the focus of the FSB in the Consultative Document and related follow-up actions should remain on the specific issue of cyber incident reporting.

Regarding cyber incident reporting, EBA CLEARING welcomes the FSB's efforts to address the duplicative cyber incident reporting requirements by different authorities, which detract resources from an institution while it is experiencing or recovering from an incident. While EBA CLEARING benefits from harmonisation at EU level in terms of the oversight of its systems, it has observed an increase in recent years in the number of non-financial authorities to whom EBA CLEARING would also have to report a cyber incident.

Regarding cyber resilience, and more specifically, threat intelligence, EBA CLEARING participates in the Cyber Information and Intelligence Sharing Initiative facilitated by the European Cyber Resilience Board (CIISI-EU). This regional forum of trusted participants allows FMI and other critical service providers in the financial industry to exchange cyber security-related information, such as on emerging or ongoing threats and risk vectors, in a closed environment. Participation and information sharing is voluntary, and the participants also have the option to submit information to the forum anonymously.

[1] 17 October 2022: https://www.fsb.org/wp-content/uploads/P171022.pdf

Recommendations (Section 3)

Are there other recommendations that could help promote greater convergence in CIR?

EBA CLEARING understands that the ultimate objective of the FSB is to achieve full convergence in cyber incident reporting. However, pending such convergence, the FSB could also encourage financial/other authorities to recognise and accept the format and content of a cyber incident report that entities must submit to their main supervisory or oversight authority. The ability of entities to provide the exact same report to multiple authorities would already alleviate some of the reporting burden they experience while trying to resolve and recover from an incident. This would free up resources that could be better used in the incident resolution.

The FSB could also include a Recommendation that financial/other authorities could contribute to the cyber resilience of the industry by providing feedback to the entities they supervise/oversee regarding the cyber incident reports they receive each quarter or each year, ensuring that the information so provided is duly anonymised. Financial/other authorities could opt to share such information to the extent it could contribute to the resilience arrangements of financial institutions and FMI, and enhance the cyber security posture of individual entities and of the industry as a whole.

Could the recommendations be revised to more effectively address the identified challenges to achieving greater convergence in CIR?

Yes.

First, as described above in the response to Question 1, EBA CLEARING considers that the FSB's Recommendations would be most effective if they focused on the specific issue of achieving convergence in the cyber incident reporting requirements imposed by financial and other authorities. However, Recommendations 9, 10 and 14 relate to individual institutions' cyber resilience arrangements, and Recommendation 15 relates to threat intelligence sharing in general, irrespective of whether an incident has occurred. In EBA CLEARING's view, these Recommendations fall outside of the scope of cyber incident reporting.

Second, there is a contradiction between Recommendation 5, which encourages authorities to select incident reporting triggers, and Recommendation 8, which would require entities to report incidents that have not (yet) reached the reporting triggers. In EBA CLEARING's view, the purpose of reporting triggers is to limit cyber incident reporting to such cyber incidents that could have a significant impact on an entity's operations, and/or the operations of other entities. In this light, it is unnecessary to also require entities to report incidents that do not meet the triggers. Near-misses or minor

incidents can be shared on a voluntary basis in a dedicated information sharing forum, to contribute to the industry's knowledge of the cyber threat landscape and overall cyber resilience.

Finally, Recommendations 2 (explore greater convergence of CIR frameworks) and 3 (adopt common reporting formats) should not only apply to financial authorities. Other public authorities, such as data protection authorities or cyber security agencies, increasingly impose cyber incident reporting requirements on FMI. The FSB should encourage such other public authorities, to the largest extent possible, to converge their requirements or adopt mutual recognition, as described above.

Common terminologies for CIR (Section 4)

The FSB should continue efforts towards promoting the uptake of common definitions by public authorities. Once public authorities are aligned as regards the definitions that apply to their cyber incident reporting frameworks, the industry can also integrate these definitions into their cyber incident reporting practices. Until then, the industry is bound by the definitions in the applicable legislation.

Format for Incident Reporting Exchange (FIRE) (Section 5)

Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater convergence in incident reporting?

EBA CLEARING agrees that the FIRE concept could – in the long term – contribute towards greater convergence in cyber incident reporting. That said, it would be important for FIRE to be adopted for operational incidents as well, to avoid divergent reporting requirements for operational and cyber incidents, as acknowledged in the Consultative Document (page 25).

In terms of the proposed FIRE format itself, EBA CLEARING supports the idea of phased reporting, in which an entity can supplement or amend initial reports as and when information becomes available.

However, EBA CLEARING considers that the "Severity Rating" category is not necessary. As per Recommendation 5, entities should only report to the authorities incidents that have met certain materiality thresholds. EBA CLEARING does not see an added value in applying additional severity ratings to the incident beyond the applicable materiality thresholds. In addition, the proposed "Lessons" category is most relevant to the overseer/supervisor of the entity and can be monitored by the overseer/supervisor in the course of its ordinary oversight/supervision of the entity, rather than in an incident report.

If FIRE is pursued, what types of organisations (other than FIs) do you think would need to be involved?

EBA CLEARING would encourage the FSB to engage with non-financial authorities, such as cyber security agencies, data protection authorities or other authorities that impose or plan to impose cyber incident reporting requirements on institutions in the financial industry.

EBA CLEARING would also encourage the FSB to engage with third party providers, so that they can be ready to support the entities they serve in their timely submission of cyber incident reports.