WORLD FEDERATION OF EXCHANGES

WFE Response to the EU Commission's Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure

Visit us at:
www.world-exchanges.org

Background

We are grateful for the opportunity to respond to the EU Commission's consultation paper on *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*.

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent over 250 market-infrastructure providers, spread across the Asia-Pacific region (~37%), EMEA (~43%) and the Americas (~21%).

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for all sorts of investors and companies wishing to raise capital and manage financial risk.

We seek outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Jonathan Pallant, Regulatory Affairs Manager: jpallant@world-exchanges.org
Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Question 1.
Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?

Answer 1:
The WFE supports policymakers and the wider industry's efforts to enhance operational resilience and to improve practices across the whole of the financial services sector. Internationally recognised common principles and standards are key to ensuring that the global markets and firms which engage with the EU, and beyond, are well positioned to understand the requirements that are made of them and to bring them up to those standards at a universal level.
The WFE believe the consideration of existing requirements and standards would be key for compliance with any such framework. It would be appropriate to consider the application and recognition of existing global frameworks, such as NIST and ISO, as well as others, which have been created under careful guidance and with dedicated resource. Use of such existing, globally recognised frameworks, which have informed CPMI-IOSCO Guidance on Cyber resilience for FMIs, ECB's Cyber Resilience Oversight Expectations for FMI and G7 Fundamental Elements of Cybersecurity for the Financial Sector, would be helpful in quickly realising and implementing those common principles across an interconnected, global financial services industry.

Question 18:
What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?

Answer 18:
Financial Market Infrastructure operates under a 2-hour RTO guidance, as per CPMI-IOSCO Principles of Financial Market Infrastructure. A 2-hour RTO guidance works well under operational disaster recovery plans. However, we consider that mandating a hard RTO for cyber scenarios under specific legislation, whilst acknowledging this has already happened in certain legislation, remains in the view of the WFE to be counterproductive. While we recognise and support the intention behind a 2-hour RTO guidance, we remain convinced that there needs to be some flexibility, to take into account particular facts and circumstances. In the wake of a cyber incident, firms may find themselves stretched between a commitment to deliver availability for customers, completing a thorough investigation of the extent of the compromise, and ensuring the integrity of seemingly untouched systems. In an ecosystem of interconnected entities, the risk of contagion should not be underestimated. Mandating a 2-hour RTO could inadvertently create the wrong incentives for the resumption of operations, at the expense of due diligence over data completeness, accuracy and validity, therefore risking the contagion to other firms and potentially causing a systemic event.

Question 21:
Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?

Answer 21:
Financial Market Infrastructures are subject to strict and detailed incident reporting requirements, which are mandated by the National Competent Authority (NCA) in the jurisdiction they operate. This regime has been in place for many years and has worked well so far. Changing the approach to create a centralised reporting structure, while seemingly an attractive option because of the uniformity, might in reality introduce problems/concerns due to a potential lack of background information or context and non-familiarity with local markets. In addition, the National Competent Authority in the jurisdiction they operate in should be the entity responsible for all incident reporting requirements to ensure simplicity in the process. Should an EU-wide system be pursued it would be important to provide clarity about any third country implications in that reporting process which may be confused or built on as part of such a system. Equally, if it is pursued, there should not be an increased, overly bureaucratic, burden on business in what is reported, nor should it result in extra resource or time implications comparative to existing practices.

Question 24:
Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?

Answer 24:
No, only high severity incidents should be reported to National Competent Authorities. Financial entities operate their incident response framework and the severity of the incidents is determined by specific criteria. For cyber incidents, there are two factors which should be considered as relevant in determining the materiality thresholds:

- Was the incident IMPACTFUL?
- Was the incident caused by a threat actor which had a TARGETED AND MALICIOUS INTENT?

Using the criteria above, only incidents that are BOTH impactful AND have targeted and malicious intent should be considered as reportable.

Question 25:
Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database?

Answer 25:
For the reasons elaborated under question 21, financial entities should report the incidents to their National Competent Authority in the primary jurisdiction they operate.

Question 26:
Should a standing mechanism to exchange incident reports among national competent authorities be set up?

Answer 26:
A standing mechanism may not be the most appropriate structure for the exchange of reporting. The WFE supports the notion of sharing information between public authorities – especially in a cross-border context. While it would be desirable for national competent authorities to exchange themes of the types of incidents they are observing in their respective jurisdictions, it would be counterproductive and run against confidentiality requirements to share, by default, the details of the incidents reported by financial entities in their respective jurisdictions. As unfiltered or unexplained content may provide a misleading picture, or result in unintended consequences, which would not arise if the NCA has autonomy over the information they provide as the 'frontline' experts for their markets.

Question 28:
Is your organisation currently subject to any ICT and security testing requirements?

Answer 28:
Members of WFE are and are supportive of a move towards harmonising their testing requirements, given the cross-border nature of the threat and the likelihood of an organisation needing to operate in more than one jurisdiction. FMIs, especially those that operate in multiple jurisdictions, are subject to multiple security testing requirements, such as CFTC Systems Safeguard Testing Regulation, Bank of England CBEST testing, Dutch National Bank TIBER NL, etc. Regulatory requirements for security testing should not be prescriptive; rather, they should be principles - and outcomes-based. This would allow firms which report to multiple regulators to meet their security testing requirements without having to perform a dedicated test, as mandated by each NCA. Furthermore, NCAs across multiple jurisdictions should work to harmonise their testing requirements, and then develop principles and requirements that firms should meet when conducting such tests. It should be left to the firms to conduct such tests, whereas NCAs should ensure that their principles are met and that findings are remediated in a timely manner, without being involved in every phase of conducting the tests. The WFE would encourage the EU to pursue opportunities to promote an international standard (i.e. globally applicable and adoptable) for security testing requirement, based on a principles- and outcomes-based approach.

Question 31:
In case of more advanced testing (e.g. TLPT), should the following apply?
(See consultation chart page 17-18)

Answer 31:
NCAs across multiple jurisdictions should harmonise their requirements for advanced testing (such as threat-led penetration testing), but responsibility should be for the National Competent Authority in their respective jurisdictions to oversee testing principles and requirements. Due to the scale and to deal with the issue of "concentration of expertise," advanced testing should be the responsibility of individual firms, while NCAs should mandate principles and requirements for testing and/or track remediation of findings, but should not be involved directly with running nor closely overseeing every phase of the tests. One major benefit of individual firms conducting their own tests is that the frequency of those tests is likely to increase, which has the benefit of frequent and increased probing of weaknesses.
Additionally, threat-led penetration testing, which more closely can be defined as Red Team adversarial simulation, should be run on live systems, while application-specific penetration tests should be run on non-production systems.

Question 39:
Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions?

Answer 39:
The finance sector has in recent years developed advanced sharing and voluntary exchange of information via industry led organisations, at a global, regional and national level. Examples include: WFE GLEX, FSISAC EU, FSCCC (in UK), etc. Given the roles of these organisations, it would seem a potentially unnecessary addition to place an extra burden on the EU to encourage this activity when it already takes place. Should it be helpful, ways of ensuring flows of information could be discussed with EU authorities so that these existing practices could be explained and detailed.

Question 48:
How would you assess the effects of the NIS Directive for your specific financial organisation? How would you assess the impact of the NIS Directive on your financial sector - taking into account the 3 specific financial sectors in its scope (credit institutions, trading venues and central clearing parties), the designation of operators of essential services and the lex specialis clause?

Answer 48:
No material effect or impact of the NIS Directive, because cybersecurity for exchanges and central counterparties already has extensive regulatory oversight. The NIS Directive appears to have given value for outlining requirements for national CERTS and CNI firms in a number of sectors. Whilst benefit can be taken from the approach and ensuring incident reporting, there is some overlap in what was happening in certain jurisdictions and additional burdens in similar reporting resulted or had to be resolved. It will be important to review the benefits of this approach and how to mitigate any new burdens.

Question 49:
Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law?

Answer 49:
Yes, it was reported that there is some duplication in reporting requirements which were originally derived from the NCA. The NCA may already have more specific requirements in their national law, to reflect the requirements of their local markets and local knowledge and experience.