DEUTSCHE BÖRSE GROUP

Gruppe Deutsche Börse

Comments on European Commission´s proposal on the review of the directive on the security of network and information systems (NIS 2.0)

Frankfurt am Main, 18 March 2021

A. General remarks

Deutsche Börse Group (DBG) appreciates the opportunity in the European Commission´s "have your say procedure" on the review of the Directive on security of network and information systems ("NIS 2.0 Directive") in order to make "Europe fit for the digital age" and the objectives of the Security union. We recognize and value the European Commission´s goal to improve the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and the protection of critical infrastructure.

DBG is operating in the area of financial markets along the complete chain of trading, clearing, settlement and custody for securities, derivatives and other financial instruments, hence is a regulated provider of regulated Financial Market Infrastructures (FMI), such as Central Security Depositories, Central Counterparties or trading venues. In its capacity as a FMI provider, DBG uses modern IT and technological solutions to operate, and service the financial sector worldwide. Currently, our entities would be in scope of the current proposals of the European Commission on NIS 2.0, the directive on the resilience of critical entities (RCE) as well as the digital operational resilience act (DORA).

Technologies are at the core of our operations, organizing regulated markets is an integral part of our regulated services. We ensure trust in markets and the efficient functioning of these markets.

Regarding new technologies, we are currently working on the use of cloud technology, AI and distributed ledger technology (DLT)/blockchain as well as automation of processes. We use these technologies in a rather gradual, granular and tested manner, hence continuing to guarantee transparency, stability and investor protection at all times.

Therefore, we support the goals of the NIS 2.0 Directive, as the security of networks and information systems is very important for our business and a precondition for the common EU Digital Market.

Please find our key positions hereunder, if you have further questions, please do not hesitate to reach out.

B. Key DBG positions

Harmonization of existing framework: we think the harmonization of the existing/future frameworks and strategies on EU / MS level should be in focus of the European Commission. Further, regulatory fragmentation referring to the digital security landscape has to be avoided.

Streamlining rules with DORA as "go-to reference" for the financial sector: We appreciate that the NIS 2.0 proposal takes the current European Commission´s proposals on DORA and RCE into account. From our point of view, DORA is intended to be a "lex specialis" for the financial sector. Therefore, DORA should be the only single reference point for financial sector entities for the issues discussed in NIS 2.0 and RCE.

In this context, we think that further clarification is needed to highlight the precedence of DORA over NIS 2.0. For example, Article 2.6 of the NIS 2.0 proposal could lead to confusion, as it describes a determination of equivalence of requirements. Therefore, we would ask for a clarification that DORA is the essential reference for the financial sector, not only in the recitals, but in the articles as well. Consequently, we would delete within Annex I the sectors 3 (banking) and 4 (financial market infrastructures) of the essential entities. This would make it clear that those entities are not in scope of NIS 2.0. Besides this, we would recommend changing the recital 13 of the proposal as follows:

> *"Regulation XXXX/XXXX of the European Parliament and of the Council16 should be considered to be a sector-specific Union legal act in relation to this Directive with regard to ~~the~~ financial sector entities. The provisions of Regulation XXXX/XXXX ~~relating to information and communications technology (ICT) risk management measures, management of ICT related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk~~ should apply to financial entities instead of those set up under this Directive. Member States should therefore not apply the provisions of this Directive ~~on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement~~ to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain ~~a strong relationship and~~ the exchange of information relating to ~~with the~~ financial sector ~~under this Directive~~. (…)".*

However, if there is a gap between DORA and NIS 2.0 with regard to scope, which would make NIS 2.0 still relevant for financial entities, we kindly ask for an explicit mentioning on the relevant provision. Finally, to streamline the used definitions and terms as well as to avoid any double regulation or potential contradictions, the developments in the legislative processes of the RCE and DORA should constantly be taken into account of legislators towards the discussion towards NIS 2.0.

"One size fits all" does not fit all and a risk based approach would be preferred: given that the NIS 2.0 Directive affects several sectors and sub-sectors, we would like to highlight that a "one size fits all" approach does not fit in any given case, as the sectors are very divergent and with varying complexities. Further, we would highly recommend a proportionality approach referring to the risk profile of the companies in scope.

Fines regime should be appropriate: We would refrain of using a fixed percentage as potential fine for infringements (Article 31.4): "(…) be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher". We would rather recommend using a risk-based formula.

Facilitate the use of new technologies: in order to facilitate the use of new technologies we would propose harmonized measures (like the use of e.g. minimum standard clauses in the cloud sector). Even highly regulated actors in the financial sector should be able to use new technologies without unproportionate burden.

Level playing field: if one function in a sector is in scope of the NIS 2.0 Directive, then all companies offering this function should be adhere to the same rules, according to a "same business, same risk, same rules".

Industry should define the state of the art of technology: due to the rapid technological changes, we would recommend a risk-based approach of the companies to fulfil their security obligations in contrast of regulatory bodies defining too prescriptive requirements, which might be soon outdated. Companies might therefore struggle to comply with such rules, and regulators might find themselves under time pressure to adjust existing requirements. Therefore, we would also recommend working closely with industry bodies and companies, this is also true for the discussion around the national cybersecurity crisis management frameworks and response plans.

Use common international standards: In order avoiding conflicting definitions and to reduce complexity, we recommend using international standards as much as possible.

DBG encourages alignment with well-established and broadly adopted best practices and industry standards in the field of coordinated vulnerability disclosure (CVD) and vulnerability handling. We strongly support alignment with these practices, as articulated in ISO international standards such as ISO27001, ISO/IEC 29147 (2018) and 30111 (2019), given the globally intertwined nature of technology and vulnerability management processes.

The risk of double regulation structures and an uneconomic bureaucratic burden: This holds particularly true for electronic communications providers and data center operators. Reporting requirements for entities must follow the 'one-stop-shop-principle'. To set up an efficient reporting channel it is crucial to specify proportionate reporting obligations and grant entities at least 72 hours for reporting an incident. A final report should not be demanded before the finalization of the forensic analysis and the introduction of measures required for ensuring business continuity.

Complexity must be reduced when it comes to reporting: Although we are well aware of the fact that cyber-related issues are not yet fully congruent with all (physical) threat vectors to critical infrastructures, the division into IT and physical security (see the RCE proposal for reference) is becoming increasingly blurred.

This development is likely to continue in the years to come. In the context of critical infrastructure protection, we encourage the Commission to also understand cybersecurity as a means to an end for safety. Subdivisions based on the motivation of the attackers are irrelevant in most cases. Cybercriminals, governmental organizations or terrorists use the same procedures and affect ultimately the same objectives to which we are committed (business continuity, readiness for response / resilience, better prevention).

Supervisory and coordinating complexity must be reduced when it comes to new public structures: Despite the desired "single point of contact" strategy within NIS 2.0, the draft creates numerous other bodies and committees as well as cross-border integration of various authorities.

This complexity should be considered and ideally reduced when further elaborating the draft. In addition, a coordinated approach by the Member States and the EU Commission would be desirable when creating new regulations.

In this way, it should be avoided that some Member States already bring national regulations in motion in the run-up to new European regulations. This approach harbors the risk of subsequent adjustments to national regulations in line with European requirements. This creates additional and avoidable effort for the legislature, executive and the obligated companies.

Streamline ICT-related incident reporting and address overlapping reporting requirements and share results: We welcome the intention that the European Commission wants to streamline and harmonize reporting duties. However, if companies report IT incidents to one competent authority, this authority should share the results/analysis/best practices with (ideally and where appropriate/necessary) supervisors and in an anonymized/aggregated way with respective market participants.

Exchange of information about threats between companies: companies should not be obliged to share information among each other until an exposed threat has been patched. This is central, as sharing threats before a patch may lead to further exposure and ultimately make it more difficult to patch.

Requirements regarding governance aspects should be reviewed: DBG recognizes that management bodies are responsible for the cybersecurity strategy of an essential or important entity (Article 17). This step will help to significantly increase the awareness for cybersecurity issues among top-level management. However, the European Commission must first publish a definition of management bodies.

In addition, requirements for training of management personnel must be limited to reasonable extent. Members of the management body do not necessarily have to undergo an advanced training in order to be able to carry out assessments of cyber security risks themselves. For this purpose, there are specialists in the companies, such as CISOs, who brief them in an adequate and comprehensible form.