EURONEXT

MEMO

Euronext position on the NIS Review

About Euronext

1. Euronext is an operator of Regulated Markets, MTFs and CSDs in 7 EEA countries. As an operator of trading venues Euronext is in scope of the current NIS Directive (Annex II)[1]. The Directive aims to boost overall levels of cybersecurity in the EU by initiating obligations for sectors vital to the EU economy. In addition, it initiated cooperation between Member States facilitating strategic cooperation and the exchange of information between Member States.

2. Euronext supports the goals set out by the NIS Directive and agrees that a **high level of cyber resilience is of great importance** for European financial markets. The NIS Directive has been instrumental in increasing awareness and facilitating cross-border intelligence sharing.

3. In the context of the review of the NIS Directive by European policymakers, Euronext believes that now is the time to take the next steps and focus on improving the structure of the NIS Directive. Below we set out our main goals, based on our experience as an operator in multiple European jurisdictions.

Maximum harmonisation

4. The NIS Directive is based on a minimum harmonisation approach. It is our experience that this approach leads to **divergences in national approaches**. We believe that divergences with regard to cybersecurity resilience are counterproductive and should be harmonised in order to boost the European level of resilience. Many financial institutions operate on a cross border level serving the EU capital market as a whole. The NIS Directive in its current approach facilitates different national approaches on what are considered to be *'appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems'* (Article 14). Having to comply with different national approaches to cybersecurity is counterintuitive as often a cybersecurity set up will apply to groups of companies and is based on one single strategy. We strongly believe – in order to boost the European level of resilience – that these requirements should be harmonised at EU level in the following areas:

With respect to standards that show compliance:

5. With respect to the level of resilience, we would support an approach where a clear framework is set by European legislators on the measures to be taken. Taking into account that measures taken are often based on international standards, we would support an approach where **certified measures** are deemed to be sufficient. That way, a clear harmonised baseline would be set, acknowledging state of the art internationally agreed solutions, thereby improving the overall level of resilience. Also, acknowledging certified measures as being compliant would set a clear level of expectation for both industry and competent authorities and would promote a harmonised cross border approach.

[1] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

With respect to reporting:

6. In addition, the implementation of the NIS Directive has led to different approaches to the reporting of incidents. In the case of a cross-border organisation, an incident occurring will likely not be limited to the borders of one Member State. As we agree that local authorities should remain close, we do not contest having to report incidents locally. However, significant progress could be made in respect of harmonising **the reporting requirements, processes, formats and time paths.**

7. When a cyber incident occurs, time is of the essence and having to spend a disproportionate amount of time on complying with multiple different forms, communication channels and timelines, takes away from time that needs to be spent on mitigating the incident. We strongly support a **single European reporting format** and communication method that would enable companies to notify local authorities in one single attempt.

Euronext supports a **harmonised set of requirements on cyber resilience**, acknowledging certified solutions as compliant with NIS.
Euronext supports a single **European reporting framework** with harmonised reporting formats and communication channels to local competent authorities.

Overlap with sectoral rules

8. In addition, we see overlapping requirements between sectoral legislation (such as MiFID II) and NIS requirements. We believe that the approach should be that – if an institution complies with the harmonised standards set by the NIS legislation – sectoral requirements should defer to those. We would support a 'tick the box approach' where compliance with NIS would satisfy sectoral regulators without having to further discuss local or national additional measures.

Euronext supports sectoral regulators **acknowledging compliance with NIS requirements to be sufficient** where it regards cyber resilience.

Importance of national authorities and their expertise

9. We support maintaining the role of local CSIRTS and competent authorities, as we believe this has a great added value to the local community where it regards information sharing and support to the sector. The level of expertise and the willingness to discuss trends, strategies and vulnerabilities by the CSIRTS and competent authorities has proven to be fruitful and positive and we would support the continued conversations.

10. We do, however, believe that the authorities should enhance international information sharing and cooperation per sector. We note that for the financial sector; efforts to further cooperate have begun and we support this. Intelligence sharing and the coordination of approaches to the sector will be vital to maximise efforts.

Euronext supports the **continued role of national competent authorities** under the framework.