Member States start discussions on content of digital operational resilience regulation proposal

The proposal for a Regulation on digital operational resilience in the EU financial sector (DORA) is making its first steps through the EU legislative process. The proposal, which would introduce a detailed legislative framework on operational resilience for financial institutions in the EU, has entered the negotiating phase in the Council. Member States are discussing different aspects of the framework through the Council Working Group meetings, the third of which took place on 28 October 2020.
We understand that the Council Working Group discussed the following issues:

1. Interaction with the NIS Directive

The Council discussed the interaction between the DORA proposal and the Network Information Systems Directive (**NIS Directive**) in relation to the requirements of the proposal on information communication technology (**ICT**) risk management and ICT-related incident reporting contained in Chapter III of the DORA proposal. Under the NIS Directive, provisions of a sector-specific EU legal act will take precedence over the NIS Directive provisions. According to the European Commission, the DORA proposal can be qualified as such a *lex specialis* since a declaration to this extent is mentioned in the proposal itself. Nevertheless, the proposal states that financial entities should remain in the ecosystem of the NIS Directive. Member States were asked to provide their views on whether this *lex specialis* approach is sufficiently considered in the proposal.

2. ICT-related incidents reporting

Currently, there are a number of parallel systems in place for the reporting of ICT-related incidents. One of the aims of the DORA proposal is to harmonise these reporting channels. Member States were asked for their views on the reporting channels introduced by the proposal, which states that incidents should be reported to the competent authority relevant to the financial institution concerned. Member States were also asked which competent authority should receive these ICT-related incident reports. In addition, Member States were asked to share their views on the interaction between incident reporting under the revised Payment Services Directive (PSD 2) and DORA. DORA would amend PSD 2 to the extent that payment service providers would have to report specific ICT-related incidents and major non-ICT related incidents under PSD 2. Some Member States are understood to be concerned that this will lead to fragmentation.

Avenue des Arts 41
1040 Brussels, Belgium
TR: 84917001473652
info@eciia.eu
ECIIA

3. Delegation of reporting requirements

Under the DORA proposal, financial institutions can delegate their ICT-related incident report to a third party after receiving approval from the relevant competent authority. Member States were asked whether they agree with this proposal, or whether the possibility to delegate these tasks should be deleted from the proposal. As a third option, a few Member States shared the view that a simple notification to the competent authority of a delegation would be sufficient.

4. Information sharing arrangements

Chapter VI of the DORA proposal provides the possibility for financial entities to set up information sharing arrangements among each other. As this could raise data protection concerns, the Presidency is understood to have asked the Council Working Group members for their views on this issue.

5. Digital operational resilience testing

Chapter IV of the DORA proposal requires financial firms to establish independent parties within or outside their firm that conduct operational resilience testing. It is understood that Member States discussed whether they agree with this requirement, or whether testing should be undertaken by external parties only, or whether at least advanced testing should be done by an external independent party. Regarding the role of the competent authority in this, the Council Working Group discussed their views on the proposal to let competent authorities identify financial entities that should perform advanced threat lead penetration testing (TLPT), or that Member States have the power to designate a more suitable national authority for this. Views are also asked on whether the proposal should explicitly refer to a TLPT framework introduced by the European Central Bank (**ECB**) in 2018. If this would be the preferred view, the possibility for the European Supervisory Authorities (**ESAs**) to specify requirements for TLPT would be deleted and replaced by the specificities of the ECB's TLPT framework. With regard to cross-border cooperation of competent authorities in charge of TLPT, questions were asked whether DORA should include a further clarification of what this supervisory cooperation would entail, or whether level 2 regulatory standards developed by the ESAs would suffice.