14 February 2023
ESMA22-106-4405

Securities and Markets Stakeholder Group

Advice to ESMA

SMSG advice to ESMA on potential practical challenges regarding the implementation of the Digital Operational Resilience Act

1 Executive Summary

On December 14, 2022, the EU co-legislators formally adopted the Digital Operational Resilience Act (DORA), consisting of a regulation (Regulation (EU 2022/2554, DORA-R) and a directive (Directive (EU) 2022/2556, DORA-D), which came into effect on January 16, 2023. DORA reflects the key role of information and communication technology (ICT) for the provision of financial services and the significant economic and systemic risk posed by the potential disruption of critical ICT systems, e.g. due to technical faults, operational error, or cybercrime. It contains a broad range of measures aimed at improving the robustness of financial-sector ICT infrastructures, covering both in-house systems and services outsourced to third-party providers (TPPs). The ESAs, mostly through the Joint Committee, have been tasked with twelve new mandates to issue technical standards, guidelines and reports within the next twelve to eighteen months. The SMSG welcomes the introduction of the DORA framework and is looking forward to supporting ESMA in the exercise of its mandate.

Concurrently with DORA, the co-legislators have adopted two directives, the Directive on Network and Information Security (Directive (EU) 2022/2555, NIS 2) and the Directive on the Resilience of Critical Entities (Directive (EU) 2022/2557, CER). Whereas NIS 2 and CER are not specific to the financial sector they apply to certain financial-sector entities, specifically credit institutions and operators of financial market infrastructures, as well as to providers of digital infrastructure and ICT services who serve the financial sector. Although DORA has been designated explicitly as a sectoral ‘lex specialis’ for the purposes of Art. 4 NIS 2 and Art. 1(3) CER, and hence takes precedence, the SMSG observes that there still are significant overlaps between these legislative frameworks, which could dilute their effectiveness unless their respective scopes of application are clearly delineated and criteria and definitions aligned as closely as practicable.

Responsibility for implementing the DORA, NIS 2 and CER frameworks is assigned to a number of different authorities, both at member-state and Union level. The effectiveness of these frameworks, in general, and DORA in particular, will depend critically on seamless cooperation between these authorities. The SMSG notes that the structures and processes to facilitate such cooperation should be designed to enable the continuous and timely exchange of information, and effective decision-making. The SMSG would support initiatives by ESMA, and its fellow ESAs, to enter into formal arrangements to create such permanent structures.

The ESAs and competent authorities should be adequately resourced to fulfil their new, significantly expanded mandates.

2 General Observations

1. The DORA framework forms part of a wider effort by the EU legislators to establish and/or harmonise standards for the resilience of critical infrastructures and services in the EU against cybersecurity incidents and threats. It overlaps, and is intended to supersede, existing guidelines issued by the ESAs and guidance from domestic competent authorities. The SMSG supports the proposed harmonisation, bearing in mind that that the duplication of rules and/or the presence of multiple, overlapping sets of rules makes it difficult for financial entities to navigate regulatory requirements and create inefficiencies and disproportionate costs of compliance.

2. While the legislative text of DORA (Level 1) appears to take in much of the existing standards and guidelines issued by the ESAs over time (Level 2 and 3), the SMSG is aware that DORA also comprises twelve new mandates for the ESAs to issue technical standards and guidelines within the next twelve to eighteen months, often dealing with very complex matters at a high level of granularity. The SMSG is mindful that there is also a substantial amount of existing member-state regulation and guidelines that will have to be taken into account in order to eliminate duplication. The SMSG recognises the challenges involved and would be happy to offer its support to ESMA in this process, where appropriate.

3. Based on the expected timeline for its implementation, DORA will become fully applicable in early 2025, i.e. 24 months after its entry into force. In view of the current position, where financial entities operate under different, sometimes diverging member-state regulations, this timetable is not without challenges. A regulatory roadmap for the implementation of DORA that addresses potential overlaps with existing EU and member-state rules, such as ESMA's Guidelines on outsourcing to cloud service providers (ESMA 50-164-4285), and allows for a smooth and comprehensive migration towards the new framework could be of great help for entities planning for the transition.

4. Concurrently with DORA, the EU co-legislators have adopted two other legislative acts of relevance, the ‘Directive on the resilience of critical entities’ (CERD) and the ‘Directive on measures for a high common level of cybersecurity across the Union’ (NIS 2). Financial market infrastructures, namely trading venues and central counterparties (CCPs), have been designated as sectors of ‘high criticality’ for the purposes of the NIS 2 and CER Directives and are liable to be designated as ‘essential’ or ‘important entities’ under NIS 2. While DORA qualifies as a ‘sector-specific Union act’ and financial institutions that are within its scope are therefore exempted from certain obligations laid down in NIS 2 (rec. 28 and Art. 4 NIS 2) these entities will still be bound by both frameworks and subject to the supervision of the respective competent authorities tasked with their implementation at the

national and EU level. The SMSG is mindful of the challenges arising from this complex regulatory architecture for both market participants and competent authorities. It supports the concerns articulated by the Chairs of the ESAs in their joint letter of 09 February 2021 to the Commission and the co-legislators (ESAs/2021/07), in particular regarding the need for streamlined and effective governance and the availability of adequate resources. In the interest of ensuring the reliable, timely and cost-effective implementation of these frameworks, reporting structures and processes for market participants should be streamlined and duplication avoided.

5. The SMSG notes that many of the EU financial entities that will be required to adopt DORA operate in tightly interconnected global markets and/or sub-contract services to ICT providers who rely on global ICT networks and infrastructure. It is important, therefore, that DORA is implemented in a way that aligns with relevant international standards, such as the CPMI-IOSCO's 'Guidance on Cyber-Resilience for FMIs', and preserves a high degree of compatibility with similar frameworks in other major jurisdictions on the basis of 'good practice', e.g. the 'NIST Cybersecurity Framework' published by the National Institute of Standards and Technology (NIST) in the U.S.

6. According to rec. 42 and Art. 4 DORA-R, the principle of proportionality should be observed in the implementation of the DORA framework. While this provision addresses, in the first instance, the practical application of DORA by financial entities the SMSG notes that it should also be considered by the ESAs when drafting standards and guidelines (Level 2 and 3), e.g. for the development of ICT risk management tools (Art. 15 and 16 DORA-R), and for the reporting of major ICT-related incidents (Art. 18 and 20(1) DORA-R).

3 ICT Risk Management

7. DORA sets out internal governance arrangements for managing and overseeing ICT risks. Art. 6(4) DORA-R, in particular, requires that the responsibility for ICT risk management should be assigned to a 'control function' with an 'appropriate level of independence'. It goes on to say that 'appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions' should be ensured, 'according to the three lines of defence model, or an internal risk management and control model.' While the wording of this provision seems to draw on the terminology and concepts of the EBA's 'Guidelines on internal governance' {EBA/GL/2021/05) it is unclear whether the co-legislators intend to prescribe a specific governance structure, e.g. with a dedicated ICT management function sitting alongside other typical 'control functions' or whether they intend to reference the general principles set out in these Guidelines. While rec. 47 DORA-R appears to support the latter reading, the SMSG would welcome further guidance from the ESAs on this issue.

4 Incident Management and Reporting

8. The SMSG welcomes the harmonisation of incident reporting within DORA, which supersedes the previous parallelism of sectoral provisions and cross-sectoral frameworks, notably NIS. Art. 19(1) DORA-R requires financial entities to report major incidents to the competent national authority under DORA (Art. 46 DORA-R) which are, in turn, required to inform the relevant ESA, the ECB, if appropriate, and the national competent authorities, 'single point of contact' or Computer Security Incident Response Teams (CSIRTs) designated under (Art. 19(6) DORA-R). The SMSG believes that further steps should be taken to standardise and streamline incident reporting for financial-sector entities. In particular, member states are required under NIS/NIS 2 to designate a 'single point of contact' for all reporting obligations under that Directive, including incident reporting (Art. 8 NIS 2). Member states are also encouraged under NIS 2 to channel reporting obligations under the CER Directive and GDPR through the same 'single point of contact', although they are not legally obliged to do so. The SMSG welcomes the establishment of 'single points of contact' and would suggest evaluating their potential use also for the purposes of sharing information provided to competent authorities under DORA.

9. The SMSG endorses the proposed centralisation of major ICT-related incident reporting (Art. 21(1) DORA-R). The establishment of a single EU Hub would facilitate information-sharing among authorities, prevent redundancies in reporting and improve effectiveness of technical and regulatory responses to cyber-risks. We note, however, that the current mandate to the ESAs is limited to the preparation of a report to be delivered within two years after DORA entered into force, and the scope of this report is limited to ICT incident reporting only. The SMSG is concerned that this approach may not be sufficiently ambitious and expedient to prevent the development of costly and cumbersome parallel structures to administer the DORA, NIS 2 and CET frameworks, which may become more difficult to build back again as time progresses.

10. The SMSG is aware that the creation of the EU Hub could lead to a situation where large amounts of potentially sensitive information are concentrated in a single place so that the EU Hub may, in due course, become a potential 'single point of failure' itself. Given the inherent risk of storing sensitive information in one centralized hub, some members of the SMSG are of the view that sensitive, company-specific information should, in principle, reside only with the national competent authorities except when this is of material relevance for the EU Hub's intended role and, in that case, preferably in anonymised form. The SMSG is also mindful, however, that national competent authorities, 'single points of contact' and CSIRTs are exposed to these same risks already today, and that the depth of resources available to member states to address them varies, sometimes considerably. The EU Hub should therefore benefit from the highest level of protection available at any given time and the SMSG believes that adequate financial and technical resources, as well as personnel, should be allocated to the ESAs to discharge this responsibility.

11. Art. 18(3) DORA-R mandates the ESAs, through the Joint Committee and in consultation with the ECB and ENISA, to develop common technical standards on taxonomies, criteria and thresholds, with a view to ensuring the consistent reporting of major ICT incidents across EU member states. In so doing, the ESAs are called upon to take into account international standards and other relevant, cross-sectoral frameworks, notably those developed by ENISA (Art. 18(4) DORA-R). ENISA, in cooperation with the Cooperation Group, is tasked with developing common incident notification templates on a cross-sectoral basis (rec. 106 NIS 2). The SMSG notes that the consistency of taxonomies, criteria and thresholds between DORA and NIS 2, in particular, will be of significant importance to guarantee the effective and seamless implementation of these frameworks. In particular, financial entities that qualify as 'essential' or 'important entities' under NIS 2 should be subject to the same set of rules as 'essential' or 'important entities' from other sectors and in-house ICT operations of financial institutions should, in general, not be treated differently from 'ICT third-party providers' (TPPs)/digital service providers (DPSs).

12. The SMSG observes that DORA does not contain explicit provisions that require entities to inform the competent authority under DORA of any loss of personal (customer) data that comes as a result of a reportable incident. This obligation exists under the general rule of Art. 33 GDPR, which generally requires all data controllers, including financial institutions, to report personal data breaches to the supervisory authority under GDPR, usually a dedicated national data protection authority. For credit institutions that are designated as 'essential' or 'important' service providers under NIS 2, competent authorities under NIS 2, i.e. national cybersecurity agencies, will also be required, in accordance with Art. 35 NIS 2, to report infringements entailing a personal data breach to the supervisory authority under GDPR (only). The SMSG is of the view that the loss of personal (customer) data by a financial institution should be considered as information that is pertinent to the mandate of the ESAs under DORA as it may expose the institution to increased risks, either directly from cyberattacks and cyberfraud by impostors using compromised customer information, and/or indirectly from compensation paid to customers as a result of such breaches. The SMSG believes that it could be conducive to the overall effectiveness of the framework if incident reports under DORA were to include, at the least, a high-level notification of personal (customer) data losses, e.g. under item (d) of Art. 18(1) DORA, which would alert competent authorities under DORA to the attendant risks. In due course, integrated reporting of incidents, with relevant reports being shared seamlessly between financial supervisors, cybersecurity and data protection authorities, as appropriate, would appear desirable.

13. Art. 19(3) DORA imposes a duty on financial institutions to inform their clients directly if a major ICT-related incident has an impact on their financial interests. This obligation stands alongside Art. 34 GDPR, which requires data controllers, including financial institutions, to inform customers of any breaches of personal data that are 'likely to result in a high risk to the rights and freedoms of natural persons'. In its 'Guidelines on personal data breach

notification under GDPR' (EDPB 09/2022) the European Data Protection Board (EDPB) notes that the risk is to be considered high if the breach 'may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.' Incidents that cause a financial loss for customers are often, but not always, accompanied by a personal data breach, and vice versa. It is important for customers whose personal data has been compromised to receive full and timely information about the nature and extent of the breach so that they can take appropriate measures. The SMSG would welcome guidance from the ESAs and the EDPB to align and integrate the process for issuing notifications under Art. 19(3) DORA and Art. 34 GDPR in all cases when both provisions apply.

5 Operational Resilience Testing

14. DORA formalises and regulates in further detail some of the ICT testing practices set out in the EBA's 2019 ICT Risk Management Guidelines (EBA/GL/2019/04). Most financial entities are obliged under Art. 26(1) DORA to carry out mandatory advanced, penetration testing at least every three years. These tests may be carried out by independent external testers, or by internal testers subject to the conditions set out in Art. 27(2) DORA-R. Every third test cycle, at least, must be conducted by an external contractor. Financial institutions that have been designated as 'significant' by the ECB must always employ independent external testers (Art. 26(8) DORA R). As a result, financial entities that are not designated as 'significant' would be exposed to external testing only once every nine years under the new rules. While the SMSG recognises that this represents a minimum requirement, and financial entities are at liberty to implement stricter testing regimes, it would still express its doubts over the adequacy of such long intervals in this complex and fast-moving environment. It notes that the degree of interconnectedness of ICT systems in the financial sector is such that a security breach at one vulnerable institution has the potential to propagate rapidly and pose a risk to the system at large, even if that institution itself is not 'significant'. Indeed, potential attackers may deliberately target smaller institutions whose defences they consider less robust. The SMSG therefore calls upon the ESAs to acknowledge this provision as a minimum requirement when formulating relevant implementation standards and guidelines, and to generally encourage shorter testing cycles and the use of independent external testers, with the possible exception of very small investment firms for proportionality considerations.

15. In order to simplify and align parallel regulatory frameworks, and to reduce the risk of regulatory arbitrage, criteria for the identification of entities required to perform mandatory threat-led penetration testing should (a) include all entities designated as 'critical third-party providers' (CTPPs) under DORA and/or 'essential' and/or 'important entities' under NIS 2; and (b) be applied consistently among member states (Art. 23(3)26(8) and 26(11) DORA). The SMSG suggests that these principles should be considered by the ESAs generally

when drafting standards and guidelines under their relevant mandates, and in their work with ENISA in the Cooperation Group.

16. The ESAs, in agreement with the ECB, are tasked with developing standards for advanced testing in accordance with the ECB's TIBER-EU frameworks (Art. 26(11) DORA). The SMSG welcomes the adoption of TIBER-EU to provide a common frame of reference for these critical, and highly sensitive tests, especially for financial entities that form part of cross-border groups. The SMSG notes, however, that (i) not all member states have adopted testing frameworks based on TIBER-EU; and (ii) there are different national implementations of TIBER-EU. The SMSG would like to emphasise the importance of a high degree of standardisation and of assuring the cross-border recognition of test results. Agreements for the mutual recognition of test results conducted in other jurisdictions outside the EU, such as CBEST in UK or tests mandated under the CFTC System Safeguards Regulation in the U.S., could be helpful in this respect, provided that the methodology meets the criteria for advanced threat-led penetration tests under DORA. The SMSG recommends that stakeholders should be consulted in the development of relevant regulatory standards and guidelines.

17. In the interest of facilitating cross-border recognition of test results, and to reduce the risk of 'regulatory arbitrage', criteria and processes for the certification and accreditation of qualified testers, internal and external, must be closely aligned across member states. The SMSG is aware of the work on EU-wide cybersecurity certification schemes, which is conducted under the auspices of ENISA. We understand, however, that these schemes are still under development. The SMSG could see value in establishing a central register of qualified external testers for the purposes of Art. 27(1) and (2) DORA, which could be administered by the ESAs.

6 Management of ICT Third-Party Risk

18. Chapter V of DORA creates a regulatory framework for the management of ICT third-party risk in the financial sector, including a dedicated oversight framework for 'critical third-party ICT service providers' (CTPPs) (Section II). The SMSG agrees with the view taken in DORA that TPPs and intra-group service providers are exposed largely to the same risks and should, as a general principle, be thus subject to the same regulatory framework. There is a caveat, in rec. 31 DORA, that financial entities may have 'a 'higher level of control' over intra-group providers, 'which is duly to be taken into account in the overall risk assessment.' The SMSG notes that this assessment should be made in a balanced way, bearing in mind that the potential benefits of tighter control of in-house units sometimes fail to materialise. This balance should also be addressed by, and incorporated into regulatory standards and guidance, where appropriate.

19. Both NIS 2 and DORA aim to provide measures for a higher common level of cybersecurity across the EU. NIS 2 will set the basis for cybersecurity risk management measures and reporting obligations across all sectors that are covered by it, such as energy, transport, banking, financial market infrastructures, digital infrastructure etc. and lay down provisions for designation of 'essential' and/or 'important entities'. DORA, on the other hand, will set uniform requirements for the security of network and information systems of entities operating in the financial sector, as well as critical third parties which provide ICT services to them and lay down provisions for designation of such 'critical ICT third-party service providers' (CTPPs).

20. There are significant differences in the methodology for designating these entities: Art. 3 NIS 2 sets out explicit conditions under which an entity is considered as 'essential', based on a size-cap rule (all medium- sized and large entities operating in the covered sectors listed in Annex I). Art. 31 DORA-R lays down a list of criteria to be taken into account by the ESAs' Joint Committee and the Oversight Forum when assessing whether an entity should be considered as CTPP or not, leaving room for possible tailoring of the requirements in certain cases (but also in a later stage throughout the adoption of delegated acts by the Commission under Article 31(6)). This could lead to legal uncertainties.

21. DORA raises the level of harmonisation on digital resilience, by introducing requirements on ICT risk management and ICT-related incident reporting that are more detailed, and stringent, than those laid down in current EU financial services legislation. It also constitutes a higher degree of harmonisation by comparison to requirements laid down in NIS 2. Accordingly, rec. 16 DORA R, rec. 28 NIS 2, and rec. 10 and 21 CER, indicate that DORA should be considered as lex specialis to NIS 2 and CER for the purposes of Art. 4 NIS 2 and Art. 1(3) CER, namely a sector-specific Union act in with regard to the financial sector entities. It is therefore of critical importance to align criteria for the designation of CTPPs under DORA with the definition of 'essential' and/or 'important entities' under NIS 2 and CER.

22. Art. 32 NIS 2, which governs the supervision and enforcement for 'essential entities', provides for member states to ensure that their competent authorities under NIS 2 cooperate with the competent authorities under DORA. In particular, it requires member states to ensure that their competent authorities under NIS 2 inform the Oversight Forum pursuant to Article 32(1) DORA-R when exercising supervisory and enforcement powers aimed at enforcing compliance of an 'essential entity' designated as a CTPP pursuant to Art. 31 DORA-R with its obligations under NIS 2. The SMSG notes that supervision of such entities, and cooperation between member states' competent authorities, would be much more efficient if all entities designated as 'essential' and/or 'important' under NIS 2, when they provide ICT services to financial entities, were explicitly designated as CTPPs under DORA. At least, the ESAs should consider including, as one of the main criteria for determining CTPP status, whether the entity in question has been designated as an

‘essential entity’ under NIS 2, and, if so, how that designation may affect those entities when providing critical ICT services to a financial entity. This would also ensure that the ‘essential entities’ framework under the proposed CER directive, which is linked to NIS 2, would also be connected to DORA. This becomes especially relevant when considering that the CER directive specifies a category of ‘entities equivalent to critical entities under the CER directive’ which member states are expected to assign to the same competent authorities as the ones designated under DORA.

23. DORA introduces a number of general principles (Art. 28 DORA) which seek to address the significant risks for financial institutions connected with the operations of ICT TPPs. The SMSG welcomes this new framework, which marks an important step towards standardising industry-wide practices and achieving a balance of risk exposure between vendors and corporate users of ICT services. The SMSG takes note, however, of the practical challenges involved in implementing these new rules.

6.1 Contracting:

- large ICT third-part service providers (TPPs) predominantly have standardised contracts that are difficult to adjust to corporate users' needs bearing in mind that users’ bargaining power is limited in many instances;

- service level agreements (SLAs) are often controlled by, and defined, in favour of TPPs, e.g. by imposing ‘default’ levels of service availability (99.5%), with additional charges levied to meet higher requirements;

- penalty clauses in case of non-compliance with SLA parameters tend to favour TPPs. Large TPPs set penalties at levels they consider acceptable to them regardless of the actual damage incurred by the end user, and always try to minimise such penalties;

- in case of incidents, TPPs tend to waive their responsibility, regardless of the actual damage incurred by the end user, and usually limit their liability to ‘gross negligence’, which is very difficult to prove;

- contracts with TPPs usually contain default clauses that assign jurisdiction to the TPPs’ home country, irrespective of where the contracted services are provided.

6.2 Legal compliance and incident reporting:

- corporate users of ICT TPPs’ services rely, to a large extent, on their reporting of incidents and sometimes find it difficult to verify the actual cause and/or extent of the incident;

- ICT TPPs tend to provide only the minimum amount of incident-related information required to comply with contractual obligations, which limits users' chances of establishing liability and pursuing legal remedies; and

- in case of any incidents, the liability of TPPs – usually limited to gross negligence – is difficult to prove and indemnification is often capped, regardless of the damage to the user.

6.3 Change Management:

- updates of outsourced services are usually actioned by the ICT TPP, while corporate users have to conform with the providers' policies and timelines;

- the same applies for emergency fixes and updates where users often have to rely on the TPP's assertion that a discovered fault or deficiency has been solved. Users often has only very limited means of verifying the TPP's assessment.

24. The SMSG notes, therefore, that the implementation of the principles set out in Art. 28 DORA will rely substantially on the ability to enforce them in a market with sometimes significant supply side concentration. This will be even more challenging where major suppliers are headquartered outside the EU.

25. The SMSG agrees that ICT-related 'exit strategies' for financial-sector entities should be sufficiently tested (Art. 28(8) DORA-R). Entities should „*expand the testing of business continuity and response and recovery plans to capture switchover scenarios between primary ICT infrastructure and redundant facilities to report to competent authorities*" (rec. 43 DORA-R). In their testing plans, financial entities should "*include scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities*" necessary to ensure that they will be capable, in the event, to restore ICT systems and data with minimum downtime and limited disruption and loss (Art. 11(6) DORA-R).

7 Information Sharing

26. As mentioned previously (3.2 above) the SMSG supports the proposed creation of a single EU Hub for incident reporting (Art. 21(1) DORA). Moreover, the SMSG is of the view that the EU Hub could, in due course, be expanded further to serve as a common platform for entities to file, and for relevant authorities to access supervisory information. The SMSG would welcome initiatives on the part of the Commission and the ESAs to investigate such a broader, more ambitious approach.

27. Sharing information about cyber threats is an established practice and an essential factor to keep industry participants and supervisors appraised of constantly evolving threat scenarios. Art. 45 DORA encourages financial entities to exchange such information on a voluntary basis, which may, or not, include the involvement of public authorities and relevant ICT TPPs. Financial entities are not generally required to report 'significant cyber threats' to national competent authorities (rec. 24 and Art. 19(2) DORA-R) and there is only a limited obligation to inform clients that are potentially affected (Art. 19(3) DORA-R). The SMSG believes that there is significant public interest in ensuring that information about significant cyber threats is made available to clients in good time, where such disclosure is possible without revealing sensitive confidential information, even if the financial entity cannot provide specific guidance on which 'appropriate protection measures' to take. Moreover, financial entities should be encouraged to share information about known threats with competent authorities which have established a secure framework for receiving such information. The SMSG is aware of the mandate assigned to ENISA to develop a European vulnerability database (rec. 62 and 63 and Art. 12(2) NIS 2) and would welcome measures by the ESAs and competent authorities under DORA to support, and contribute to this effort.

8 Supervisory Structures and Processes

28. DORA, in conjunction with the NIS 2 and CER Directives, establishes a complex, multi-layered governance framework which combines vertical/sectoral and horizontal/cross-sectoral mandates. Under DORA, responsibilities are allocated along sectoral lines among national competent authorities, the ECB and the ESAs (Art. 46 DORA-R). Units belonging to large financial groups whose activities span more than one sector may fall under the purview of different competent authorities, even though they may rely on the same provider(s) of ICT services, e.g. a central in-house ICT unit. Competencies under NIS 2 are assigned to (one or more) national competent authorities, including a 'single point of contact', charged with supervising the implementation of the Directive (Art. 8 NIS 2), and one or more CSIRTs for the specific purpose of incident handling. Coordination between national competent authorities under DORA and the structures and authorities established under NIS/NIS 2 is expected to take place primarily in the Cooperation Group established under Art. 14 NIS 2, in which national competent authorities and the ESAs are entitled to participate upon request (Art. 47(1) DORA-R). The SMSG notes that there appears to be no mechanism in the proposed Level 1 legislation to facilitate continuous, day-to-day cooperation between competent authorities under the two frameworks, especially when tasked with supervising the same 'essential' or 'important' financial-sector entity. The SMSG would encourage the ESAs and NCAs under DORA to establish permanent structures and processes supporting the (NIS 2) Cooperation Group in order to promote information-sharing on a seamless and continuous basis (Art. 47(1) DORA-R and Art. 14 NIS 2)

29. DORA confers new tasks and responsibilities upon ESMA and the other ESAs. These new mandates are likely to require additional capacities and, in some instances, entirely new skill sets that may be in short supply and difficult to develop internally. The SMSG supports the suggestion by the ESAs in their joint letter of February 2021 to create a joint technical unit supporting the Oversight Forum to leverage relevant skills and capacities. The SMSG is of the view that the creation of a permanent pool of skilled personnel dedicated to the implementation of DORA, could contribute significantly to the development of critical in-house expertise and a high degree of continuity and convergence. Such an approach would not contradict but rather complement the use of independent experts, as envisaged in Art. 32(4) and (6) DORA-R.

30. The SMSG observes that the involvement of the European Data Protection Board (EDPB) in the Cooperation Group under NIS 2 is recommended only and remains at the sole discretion of the Cooperation Group (rec. 66 NIS 2). Bearing in mind that ICT incidents are often accompanied by a loss of customer data, and the potential extent and gravity of such personal data breaches, the SMSG believe that the EDPB should be involved in this forum more prominently, possibly on a regular basis.

This advice will be published on the Securities and Markets Stakeholder Group section of ESMA's website.

Adopted on 27 January 2023.

[signed]	[signed]
Veerle Colaert Chair Securities and Markets Stakeholder Group	Christian M. Stiefmueller Rapporteur