BSG own initiative paper

BSG 2023 03

5 May 2023

BANKING STAKEHOLDER GROUP

BSG own initiative paper on **DORA**

Main challenges and recommendations

1. EXECUTIVE SUMMARY

1. The BSG welcomes the DORA legislative package which establishes a comprehensive framework on digital operational resilience for EU financial entities by streamlining and strengthening the existing patchwork of relevant provisions across EU financial services legislation.
2. 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).
3. The ESAs, mostly through the Joint Committee, have been tasked with 16 new mandates to issue technical standards, guidelines and reports within the next twelve to eighteen months.
4. The BSG welcomes the introduction of the DORA framework and is looking forward to supporting the EBA in the exercise of its mandate.
5. The objective of the Own Initiative Paper is to provide early advice and recommendations to the EBA (and to the other ESAs) on the macro challenges that DORA will bring for regulators, financial institutions, ICT service providers and consumers.

2. INTRODUCTION

6. The European Commission adopted a Digital Finance Package on 24 September 2020, which includes a proposal for a Regulation on “digital operational resilience for the financial sector” (DORA), accompanied by a Directive.

7. The overall objective of the DORA legislative package is to make sure the financial sector in Europe is able to effectively manage ICT and cybersecurity risk, including when arising from a third-party provider, and to stay resilient through a severe operational disruption.
8. The DORA Regulation aims to streamline and upgrade existing rules on:
    - ICT Governance and the management of ICT risks (**Chapter II**);
    - the management, classification and reporting of ICT-related incidents (**Chapter III**);

    and to introduce new requirements where gaps exist, particularly with respect to:
    - digital operational resilience testing (**Chapter IV**);
    - management of ICT third-party risks and regulation and oversight of 'critical third-party ICT service providers' (CTPPs) (**Chapter V**);
    - information sharing (**Chapter VI**); and;
    - the tools the financial supervisors need to fulfil their mandate to contain financial instability stemming from those ICT vulnerabilities (**Chapter VII**).

9. The DORA Directive is then tasked with amendments to financial services directives to introduce cross-references to the DORA Regulation and to update empowerments for technical standards.

3. GENERAL OBSERVATIONS

DORA and the current regulatory framework for resilience of critical infrastructures

10. 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.
11. Two other legislative acts of relevance, the "Directive on the resilience of critical entities" (CER Directive) and the "Directive on measures for a high common level of cybersecurity across the Union" (NIS 2 Directive), have been adopted. The banking sector has been designated as a "sector of high criticality" for the purposes of the NIS 2 and CER Directives and credit institutions are liable to be designated as "essential" or "important entities" under NIS 2. While DORA qualifies as a "sector-specific Union act" (*lex specialis*) and financial institutions that are within its scope are therefore exempted from certain obligations laid down in NIS 2 (recital 13 and Art. 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. This means that potential overlaps still exist and will need to be addressed to avoid duplication.
12. The BSG 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 for competent authorities and the availability of adequate resources. In the interest of ensuring the reliable, timely and cost-effective implementation of this framework, reporting structures and processes for market participants should be streamlined and duplication avoided.

DORA as part of broader management of operational risk

13. DORA complements the prudential (operational risk) framework in the Capital Requirements Regulation (CRR II) and Directive (CRD V), which focuses on ensuring that banks are capable, ex-post, to withstand the economic and financial impact of a major ICT breach or failure. DORA, by contrast, introduces harmonised operational structures and processes to identify, manage and mitigate ICT risk, with a focus on prevention and recovery. It is important, in our view, to ensure that these two frameworks are applied in a consistent and holistic way within the Supervisory Review and Evaluation Process (SREP).
14. For payment service providers (PSPs), DORA expands on, and partly overlaps with, existing provisions on operational and ICT risk management in the Second Payments Directive (PSD 2), notably Arts. 95-98 PSD 2. In particular, incident reporting by PSPs, which is governed currently by Art. 96 PSD 2, EBA's 'Revised Guidelines on major incident reporting' (EBA/GL/2021/03) and implementing national legislation, will be subsumed into DORA (recitals 23 and 42 and Chapter III DORA). The BSG is of the view that practical insights and proven practices from the implementation of incident reporting under PSD 2 could be transferable to the new framework. In some respects, this learning may support a degree of continuity maintained, including the alignment with increased materiality thresholds. In others, the learning will indicate that work is likely to be needed to ensure that reporting is commensurate with the level of threat and incidents actually experienced and given due supervisory focus where this is not the case.
15. For both financial institutions and customers, it is important to remember that operational resilience is not only related to the management of external shocks and events, such as cyber-resilience, but also a function of the financial institutions' own management of technology and systems, and of change in such systems. It is important to consider in this regard the prevention of outages, the potential impacts of data loss and the timely and orderly recovery and minimisation of harm from such incidents when they arise. The BSG is keen to ensure that this is a focus of attention in the preparation of technical standards and implementation and that in determining criteria relating to criticality consideration is given to the impact on customers of the non-availability or other problems in using the service. For retail clients, the non-availability of a current account or payment account effectively makes everyday life impractical, which is not the case for all financial services, regardless of whether data is compromised. This significance should be reflected in the criteria relating to criticality, such as the classification of serious ICT-related incidents under Article 18, firms' assessments of criteria for triggering incident response processes, and the content of response and recovery plans.
16. Even though it brings the practical challenges discussed further below, we welcome the fact that the DORA framework provides for consideration of the whole financial sector. This is important given the interconnectedness between the different sectors and the likelihood of some external threats being relevant to all types of entities.
17. In recognition of the importance of the DORA framework and its broad scope, the BSG aims to contribute actively to the Level 2 work and to do so as far as possible in collaboration with our counterpart stakeholder groups in ESMA and EIOPA and also taking account of contributions from ENISA and other relevant user groups and stakeholders (i.e., ICT third party service providers).

DORA and the international approaches to operational resilience

18. The effectiveness of the DORA framework will depend on the ability of financial institutions to capture, analyse, aggregate and report data on digital operational risks in a timely, accurate and consistent manner. At the international level, the Basel Committee on Banking Supervision (BCBS) issued the "Principles for effective risk data aggregation and risk reporting" (BCBS 239) in January 2013. Principle 2 states that banks *should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis*. Reviews by the ECB and the BCBS, in May 2018 and April 2020, respectively, found that a significant number of the banking groups under review (mainly global and other systemically important institutions (G/O-SIIs)) were still largely non-compliant with BCBS 239. A high degree of operational resilience, especially among institutions, is of paramount importance for the stability of the banking sector at large. The BSG welcomes the contribution that DORA is likely to make as a step towards compliance with relevant international standards, in general, and BCBS 239, in particular. The BSG sees the implementation of DORA as an opportunity to reinforce the need for action to deliver the capabilities required under BCBS 239, and notes that where financial institutions do have such risk data aggregation capabilities in place their ability to meet DORA requirements and convince supervisors that they are adequately assessing and managing operational risk is likely to be enhanced.
19. The BCBS published the "Principles for Operational Resilience" in 2021 to strengthen operational resilience by increasing international engagement and promoting greater cross-sectoral collaboration to build on the work already implemented by several jurisdictions and standard-setting bodies. The principles include ICT-related risks to operational resilience and also cover other potential causes of operational disruption, whether internal/external and ICT-related or not.
20. In October 2021, the IOSCO published a revised "Principles on Outsourcing", which established expectations for regulated entities that outsource tasks and briefly addressed the impact of COVID-19 on outsourcing operational resilience.
21. In July 2022, it was published a Joint Statement from the UK-US Financial Regulatory Working Group where they addressed the importance of digital operational resilience for "critical" third-party providers that provide services across borders and sectors. The regulators recognized that there would be value in developing shared international approaches to identifying critical services and providers, and to collaborate on how to address any disruptions in their services.
22. The Financial Stability Board (FSB), following a G20 request, issued a consultation on Achieving Greater Convergence in Cyber Incident Reporting, acknowledging that timely and precise information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability. The goal is that financial institutions operating across borders are not subject to multiple conflicting regimes. Also, the FSB recently completed a consultation on the "Regulatory and Supervisory Issues Relating to Outsourcing and Third-party Relationships".
23. The BSG is of the view that all these international initiatives should be taken into consideration when developing the Level 2 work to ensure consistency with international benchmarks. Additionally, the technical standards should reflect and enable cross-border firms to adopt a consistent approach to digital operational resilience group-wide and adapt it to each jurisdiction as necessary.

4. MAIN CHALLENGES AND RECOMMENDATIONS

4.1. CO-ORDINATION BETWEEN AUTHORITIES AND EFFICIENCY

24. Given the pervasive and cross-cutting nature of the risks to digital operational resilience that DORA intends to address, the BSG welcomes the fact that DORA addresses the whole financial sector, while enabling tailoring to the specific risks of different business models and activities and that significant emphasis is placed on collaboration between all the different authorities with a role to play. This should make the legislation both more effective and less burdensome for those who have to comply with it.
25. However, the landscape of bodies who will need to be involved in developing technical standards and in implementing and supervising the regime is extremely complex and cumbersome. 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.
26. Under DORA, responsibilities are allocated along sectoral lines among national competent authorities, the ECB and the ESAs (Art. 46 DORA). 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. an intra-group ICT unit. There are also complex calculations for determining, for example, which ESA is responsible for a particular technology provider.
27. 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. 12 NIS 2, in which national competent authorities and the ESAs are entitled to participate upon request (Art. 47 DORA).
28. The BSG also 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. 34 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 BSG believes that the EDPB should be involved in this forum more prominently, possibly on a regular basis.
29. The BSG notes that there appears to be no mechanism in the proposed Level 1 legislation that would facilitate continuous, day-to-day cooperation between competent authorities under the NIS2 and DORA frameworks, especially when tasked with supervising the same "essential" or "important" entity. This is particularly important because in addition to collaboration within the Union, it will be highly beneficial for both financial services providers and consumers if there are efforts to agree common approaches and practical collaboration with counterparts in key third countries. It will also help financial services providers operating in multiple jurisdictions to streamline policies and procedures, and it will help consumers because the threats are rarely limited to the borders of the Union.

4.2. A COHERENT REGULATORY AND SUPERVISORY APPROACH TO OPERATIONAL RESILIENCE

30. It is important that the ESAs, the ECB and national competent authorities work towards a holistic and common approach to the identification and management of risks to digital operational resilience and that these are embedded in an approach which takes account of other aspects of operational resilience.
31. This means that:
    - Attention will need to be paid to prevention, recovery and harm reduction when incidents arise;
    - Consideration will need to be given to a range of potential drivers or triggers of harm, including poor capacity planning or change management by financial institutions as well as external events such as cyber-events or physical shocks;
    - Financial institutions will need in some situations to be partners in addressing risk but may also be potential sources of risk and relationships with supervisory authorities will need to allow for open communication in such cases;
    - Complementary and coherent use of prudential tools and other supervisory tools will be needed, including tools to support remediation for customers impacted by serious ICT-related incidents.
32. The BSG would encourage the ESAs to make use of their relevant competencies and instruments to promote both regulatory and supervisory convergence and to work closely with the ECB as well as NCAs to achieve this. In addition to the formal mandates already given by the Level 1, we encourage the ESAs to consider establishing common risk-based supervisory priorities on digital operational resilience in the early years of the regime, supported by extensive collaboration and underpinned where appropriate by periodic peer review.
33. It will also be useful to think creatively about situations where some authorities within the European Union may want to pool or delegate mandates in order to make the best use of resources in a highly complex area and reduce unnecessary duplication of resource or effort. This could be facilitated by the development of a central infrastructure.
34. As an example, the BSG endorses the proposed centralisation of major ICT-related incident reporting (Art. 21 DORA). 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 only limited to the preparation of a report to be delivered within two years after DORA entered into force, and the scope of this report covers ICT incident reporting only. The BSG 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 CER frameworks, which may become more difficult to build back again as time progresses. The BSG is of the view that a single EU Hub could, in due course, serve as a common platform for entities to file and share, and for relevant authorities to access supervisory information and would welcome initiatives on the part of the Commission and the ESAs to investigate such a broader, more ambitious approach.
35. Sharing information about cyber threats is an essential factor to keep industry participants and supervisors appraised of constantly evolving threat scenarios. Art. 19 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

(recital 24 and Art. 19 DORA) and there is only a limited obligation to inform clients that are potentially affected. The BSG believes that there is significant public interest in ensuring that information about significant cyber threats is made available to clients in good time, 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. The BSG is aware of the mandate assigned to ENISA to develop a European vulnerability database (recital 62 and 63 and Art. 12 NIS 2) and would welcome measures by the ESAs and competent authorities under DORA to support and contribute to this effort.

36. Another important aspect of the approach will be to incentivize financial institutions to acknowledge and manage risks to digital operational resilience. In this regard the style and focus in supervision is critical, to avoid that firms could downplay the likelihood or impact of experiencing operational challenges. This means, for example, that it is important to scrutinise firms that do not report experiencing cyber-incidents, as well as those that do, given that the fact of reporting may indicate better controls and a more open relationship with supervisory authorities in the reporting firm.
37. In this regard it will also be important to consider the complementarity of DORA with the prudential framework. The DORA Directive inserts a new item (b) in Art. 97(1) CRD IV, which mandates competent authorities to incorporate the results of digital operational resilience testing under DORA into the supervisory review and evaluation process (SREP). Material shortcomings in ICT security that are identified as part of resilience testing may, in due course, lead to breaches that could expose institutions to significant financial liabilities. As part of its mandate under Art. 107(3) CRD IV, the EBA has issued Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (EBA/GL/2017/05). It will be necessary to keep a balance between incentivising firms to report incidents and assessing how incidents, and ICT-related vulnerabilities they may be connected to, are taken into consideration as part of the SREP. It will also be important to ensure that non-security related ICT incidents due to factors such as poor capacity planning or change management are taken into account in the SREP. Furthermore, the rightly-increased focus on ICT-related risks should avoid giving the impression that ICT is the only source of risk to operational resilience or the only factor to be considered in determining the adequacy of response and recovery to incidents.

4.3. CAPACITY BUILDING AND BEST USE OF RESOURCES

38. The BSG is mindful of the challenges arising from this complex regulatory architecture and for the highly technical nature of the issues on scope, both for market participants and competent authorities. We support 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), regarding the need for adequate resources, given the specialist expertise and additional infrastructure required.
39. But financial entities will also need to ensure they have sufficient internal resources to implement the assessments, mapping, testing and other additional actions the new regime demands. Employees may need to be trained to ensure they have the skills and knowledge, and it will be important to ensure senior management are sufficiently informed and trained to enable them to provide the requisite level of oversight of the firm's digital operational resilience.

40. The challenge is even bigger considering the skills gaps and the shortage of talent in these areas for both market participants and authorities.
41. There needs to be more investment in technical skills and training in ICT related issues and in the intersections between technical skills in ICT and policy making and supervision.
42. Taking into account the challenges stated above, the BSG encourages the ESAs to develop a single, shared pool of staff with the necessary expertise to develop the detailed implementing measures under DORA and carry out the resultant supervision.
43. Wherever legally possible, the ESAs and NCAs should delegate responsibilities to this single pool and should have a single line for management oversight to reduce duplication and complexity.
44. Even with this pooling, we do not think it is feasible for the ESAs to deliver the regime without access to additional staff and resource and therefore recommend that a budgetary increase is granted for this work as soon as possible.
45. In order to avoid duplication and to get the most of the combined resources between competent authorities under the NIS2 and DORA frameworks, the BSG is of the view that it is important to get the right governance for the collaborative effort in place from the start.

4.4. ICT RISK MANAGEMENT AND INTERNAL GOVERNANCE

46. DORA sets out internal governance arrangements for managing and overseeing ICT risks. Art. 6(4) DORA, in particular, requires appropriate segregation of ICT management functions. 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 risk management function sitting alongside other typical 'control functions' or whether they intend to reference the general principles set out in these Guidelines, leaving financial institutions a degree of discretionary latitude as to their implementation.
47. The BSG believes that further clarification would be needed to ensure that these rules are consistently applied and understood by financial service providers. Furthermore, the BSG highlights that these new functions will need adequate resources and capacity building for a new set of skills (for instance: "Compliance and Risk functions do not normally possess sufficient knowledge, skills and expertise in ICT risk"). Emphasis should be placed on ensuring that each line of defence has the appropriate independence and expertise to perform its intended function. It is also important to ensure that an emphasis on ICT risk management as a distinct consideration does not lead to an unhelpful disjunction between governance of ICT risk and broader operational risk given likely interdependences between them.

4.5. THE OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD PARTY SERVICE PROVIDERS (TPPs)

48. 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 BSG 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 recital 31 of the DORA regulation, that financial entities 'might' have 'a 'higher level of control'

over intra-group providers, 'which is duly to be taken into account in the overall risk assessment.' The BSG 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 in practice due to other operational risk factors, such as agency problems and moral hazard.

49. It is important to consider the interconnections between the implementation of the DORA regulatory regime for financial institutions and the regime for technology providers. These need to be taken into account in developing the Level 2 measures, in designing the oversight regime for technology providers, and in delivering effective supervision and enforcement of both regimes.
50. Financial institutions use ICT TPPs for a variety of reasons, e.g. to access innovative technologies offered 'as a service' as an alternative for outdated legacy ICT infrastructure, or to source products and services that they cannot economically develop or maintain in-house. 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 BSG 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 BSG takes note, however, of the practical challenges involved in implementing these new rules.
51. With respect to contracting, the BSG would like to point out that:
    - major ICT TPPs tend to use standardised contracts that are often difficult to adjust bearing in mind that corporate users' bargaining power is limited in many instances;
    - contracts with major ICT TPPs are usually drawn up under the home jurisdiction of the supplier even if the service is provided in a different jurisdiction; and
    - major ICT TPPs have a significant level of control in defining industry-wide standards for service level agreements (SLAs), including guaranteed levels of service, indemnification and penalty clauses in case of non-compliance.
52. With respect to incident reporting, the BSG observes that:
    - 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; 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.
    - Similar challenges exist, for instance, in connection with change management, especially where outsourced services sit alongside, and interact with, in-house services:
    - 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.

53. The BSG notes, therefore, that financial institutions' 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.
54. The implications of the above are that:
    54.1. The design of the oversight regime for technology providers needs to pay close attention to the areas where financial institution clients currently face challenges in getting co-operation from TPPs;
    54.2. The effectiveness of the TPP oversight regime will affect the likelihood that financial institutions can deliver effectively on their obligations under Article 28, and a mechanism for taking into account the supervisory assessment of the relevant TPPs in the assessment of the financial institutions may be needed;
    54.3. Collaboration with competition authorities may be needed to ensure that effective remedies are available to financial institutions where there is a persistent difficulty with a critical TPP.
55. In addition, careful consideration needs to be given to the impact of any sanction envisaged or imposed under the oversight regime on the operational resilience of the financial institutions which rely on it, particularly for SIFIs.

4.6. THE NEED FOR DEVELOPING INTERNATIONAL STANDARDS – INCIDENT REPORTING

56. The BSG stresses the importance of designing global standards to achieve an internationally consistent and coherent digital operational resilience framework. Currently, some requirements are insufficiently harmonized and use different terminology and timeframes at international level. Consequently, there is a very real risk that internationally active firms will struggle to achieve resilience by design and substitutability in their service provision. Given the cross-border service delivery interdependencies for financial firms today, the resilience of a firm's services in one jurisdiction will often depend on the supporting assets or processes located in other jurisdictions.
57. For instance, Art. 19 DORA requires financial institutions to report major ICT-related incidents to the competent national authority under DORA 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). In order to streamline supervisory activities between the competent authorities, and to minimise the administrative burden for the entities concerned, member states are required under NIS 2 to designate a 'single point of contact' for all reporting obligations under that Directive, including incident reporting (Art. 8.3 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 BSG 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.
58. Art. 18.3 DORA 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(3) DORA). ENISA, in cooperation with the Cooperation Group, is tasked with developing common incident notification templates on a cross-sectoral basis (rec. 56 NIS 2).

59. The BSG welcomes the harmonisation of incident reporting within DORA, which supersedes the previous parallelism of sectoral and cross-sectoral frameworks, especially PSD 2 and NIS/NIS 2. The BSG believes that further steps should be taken to standardise and streamline incident reporting for financial institutions, in particular when these firms act on a cross-border basis.
60. In 2021 the Institute of International Finance published a paper on the 'Importance of more effective cyber incident reporting'. The paper highlights that cyber incident reporting is less effective than it can be due to ambiguity around how firms and authorities define what constitutes a cyber incident or a "major" incident. These differences are intensified by insufficient information-sharing, including from authorities to firms, and inadequate cross-border cooperation and collaboration.
61. The BSG is of the view that there could be lessons learnt from the area of AML in order to calibrate reporting adequately and avoid both over reporting of low-quality information (crying wolf effect) or under reporting.
62. In a paper published by the FATF in 2021, "Opportunities and challenges of new technologies for AML/CFT", that Artificial intelligence (AI) and machine learning (ML) technology-based solutions applied to big data can strengthen ongoing monitoring and reporting. The BSG considers that attention should be paid to both RegTech and SupTech, considering that they can improve the effectiveness of compliance and reporting in this relevant area.

4.7. ATTAINING AN ADEQUATE LEVEL OF STAKEHOLDER DIALOGUE AND COLLABORATION

63. DORA has a broad scope and applies to most of the regulated financial institutions in the European Union, including *inter alia* banks, insurance companies and intermediaries, PSPs/EMIs, investment firms, pension funds, crypto-asset service providers, crowdfunding service providers, fund managers and ICT third-party service providers. In this context, attaining and adequate level of stakeholder engagement can be complex, as it involves effectively communicating with and involving a diverse group of stakeholders with different interests and perspectives. Furthermore, the existing ESA stakeholder groups were not constituted in such a way as to include TPPs.
64. The BSG is of the opinion that given the complex regulatory architecture that underpins DORA, the technicality of the issues at stake and the cross-sectoral and international nature of the work involved, it is advisable to find a new forum where stakeholders from different sectors of the digital supply chain can exchange and discuss information between themselves and with competent authorities (both at European level and internationally).

4.8. BUILDING DETAILED RISK TAXONOMIES

65. DORA is the first piece of legislation at the European level harmonizing the topic of digital operational resilience and cybersecurity for financial services. It will open-up opportunities for the EU to take a leading role in the field of digital financial services and to set global standards.
66. To achieve a level playing field, supervisory convergence and consistent industry practices, sufficiently detailed and internationally consistent ICT risk taxonomies should be developed, e.g. by building on existing work such as the FSB's cyber lexicon and relevant ISO standards. The BSG is of the view that an incident classification should have a common language and criteria both at European and international level. A unique taxonomy will be used for the event

detection and in the impact analysis. This could represent the starting point to define an incident reporting standard. A common taxonomy promotes consistency and alignment across all markets. This approach could bring benefits for information sharing and to ease the collaboration among institutions and authorities.

67. The BSG highlights that the consistency of taxonomies, criteria and thresholds between DORA and NIS 2 in particular, where this can be achieved without negating the purpose of the respective provisions, will be of significant importance to guarantee the consistent and seamless implementation of these frameworks. For instance, financial institutions 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 not be treated differently from TPPs.
68. The ESAs should build common and detailed ICT risk taxonomies to guarantee consistent industry practices and a level playing field, while allowing for evolving circumstances and unforeseen issues. For instance, we consider that the ICT risk taxonomy provided in the "EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)" is not detailed enough to guarantee supervisory convergence and should be amended accordingly.

4.9. TESTING: ADOPTION AND EVOLUTION OF THE TIBER EU FRAMEWORK

69. Financial entities, other than microenterprises and small and non-interconnected entities (Art. 16 DORA), are obliged under Art. 26.1 DORA to carry out mandatory advanced, threat-led penetration testing (TLPT) 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. Every third test cycle, at least, must be conducted by an external contractor (Art. 27.2 DORA). As a result, financial entities would be exposed to external TLPT only once every nine years under the new rules. While the BSG 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. The BSG would therefore call upon the ESAs to acknowledge this provision as a bare minimum requirement when formulating relevant implementation standards and guidelines, and to encourage shorter testing cycles.
70. DORA aims to align advanced, TLPT and processes across member states with the TIBER-EU framework (Art. 26.11 DORA). It would be critical to build on firms' experience of reporting and supervision under PSD 2, and on the experience of the TIBER-EU framework for penetration testing which at least some countries have implemented and is the basis for the new regulations. The BSG stresses the importance to ensure alignment/avoid duplication with existing legislation (e.g. 'lex specialis' for general cyber regime) and also ensure that there is scope for TIBER-EU to evolve in the light of new developments.
71. The BSG highlights the importance to ensure that criteria for the identification of entities required to perform mandatory threat-led penetration testing (i) include all entities designated as 'critical third party providers' (CTPPs) under DORA and/or 'essential' and/or 'important entities' under NIS 2; and (ii) are applied consistently among member states – Art. 23(3) and 23(4) DORA).]

72. DORA sets out a list of specific requirements for testers to be eligible to carry out threat-led penetration testing on financial entities (Art.27 DORA). The BSG notes, however, that there are currently no EU-wide testers certified by an accreditation body in a Member State or that adhere to formal codes of conduct or ethical frameworks. The BSG could see material benefits in aligning certification and accreditation criteria and processes for qualified internal and external testers across member states (Art. 27 DORA). The BSG is aware of the work, spearheaded by ENISA, to develop harmonised EU cybersecurity certification frameworks. Whereas the frameworks currently under development focus on other areas, such as ICT products and cloud services.
73. Furthermore, the BSG considers that there are responsibilities 'not to be taken lightly': providers of independent external testing services must be substantive enough to bear potentially sizable liability claims in the event of error but care must be taken equally to (i) avoid concentration in the hands of only a few large providers, and/or (ii) prevent conflicts of interest when a variety of services is provided by the same large firm, which could end up 'marking its own homework'. Finally, ensuring a suitable depth of resources within providers has historically been a problem, with some firms reporting needing to pause their TLPT while their chosen provider recruits new qualified testers. This situation may worsen significantly as DORA enters into force and the number of tests being conducted increases substantially. Ensuring a smooth and consistent certification process that enables efficient on-boarding of qualified testers will be important to the effectiveness of DORA's TLPT requirements.
74. The BSG could see value in exploring the establishment of a central, EU wide, public register – held by the ESAs – of qualified external testers certified by accreditation bodies in the member states, e.g. the National Cybersecurity Certification Authorities (NCCAs), in accordance with harmonised criteria and standards.

4.10. IMPACT ON CONSUMERS

75. It is important to acknowledge the different kinds of impact that failures in digital operational resilience can have on consumers, mainly:
    - Lack of service availability as a result of unplanned outages (as distinct from occasional planned service maintenance) can cause real distress, particularly where it means consumers cannot access funds. For some the reliance on digital service availability has been significantly increased by diminished availability, use and acceptance of cash.
    - Loss of data clearly brings potential financial loss as well as distress arising from loss of privacy.
76. As discussed above, we consider that these aspects should be taken into account in considering criticality, particularly in relation to current accounts and similar payment accounts.
77. The nature of these impacts is that they cannot be fully put right after the event, so an emphasis on prevention is key, and on effective handling of incidents where they do arise – not just punishment for the event – is also important. It would therefore be helpful for common expectations to be set among competent authorities in relation to handling events so as to so as to reduce and remediate harm, and for those expectations to be applied through the common, risk-based supervisory priorities discussed above.
78. The BSG 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. 32 NIS 2, to report infringements entailing a personal data breach to the supervisory authority under GDPR (only).

79. Art. 17 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.'*
80. The BSG 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, e.g. from cyberattacks and cyberfraud by impostors using compromised customer information, and/or from compensation paid to customers as a result of such breaches. The BSG 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. 16(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.
81. 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 BSG would welcome guidance from ESAs and the EDPB to align and integrate the process for issuing notifications under Art. 17 DORA and Art. 34 GDPR in all cases when both provisions apply.