FIA.org

FIA final response to EBA SREP Guidelines consultation

The Futures Industry Association (FIA) is the leading global trade organization for the futures, options and centrally cleared derivatives markets. FIA's member firms include clearing firms, exchanges, clearinghouses, and trading and commercial firms that operate in the exchange-traded derivatives markets.

FIA Members appreciate the opportunity to provide feedback to the European Banking Authority (EBA) Consultation Paper on the Draft Guidelines on common procedure and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (the "**SREP Guidelines**"). In our response, FIA highlights issues for consideration by the EBA for the SREP Guidelines, with the aim of increasing proportionality and increase alignment with existing EU regulatory frameworks in the Operational Resilience space. FIA stands ready to give further feedback as requested by the EBA on the issues raised in this response.

Member comments:

The introduction of Operational Resilience as a broad concept in the SREP Guidelines does not align with the EU regulatory framework. While certain specific elements are included within the EU regulatory framework, such as DORA and the EBA Draft Guidelines on the sound management of third-party risk, these do not fully cover an holistic concept of 'Operational Resilience' as expressed in the SREP Guidelines.

The requirements expressed in DORA are specifically targeted at 'Digital Operational Resilience'. The third-party risk management requirements similarly have a clear and specific focus, as set out in DORA Articles 28-30, rather than providing a framework for a holistic approach to Operational Resilience that extends beyond the digital and ICT- specific scope.

Similarly, while some jurisdictions, such as Ireland, do have an Operational Resilience framework, the absence of a clear and consistent approach across member states will lead to fragmented and varying implementations, conflicting with the aim of harmonisation advocated by European authorities and the EU legislator..

Our members do not consider the SREP Guidelines as an appropriate approach to develop and implement what amounts to a far-reaching, broad and highly demanding set of supervisory expectations. A change of this scope would likely justify separate, specific consultation with industry and possibly even require Commission Regulation to form the basis of it.

These concerns are further compounded by the extremely broad and loose definition of 'Operational Resilience' leveraged by the EBA, which also deviates significantly from existing definitions of operational resilience in jurisdictions such as Ireland.

Members would propose that references to Operational Resilience are restated to be framed around Digital Operational Resilience, to ensure that it is aligned with the regulatory framework. Some specific comments include:

- Paragraph 68.c. refers to a competent authority's assessment of an institution's "operational resilience, by reviewing the institution's operational resilience framework". In line with our wider comments, there is no current regulatory requirement for institutions to have a holistic operational resilience framework in place.

- Paragraph 92.g. refers to "appropriate and consistent links between the business strategy, risk strategy, digital operational resilience strategy". During the development of the technical standards under DORA, it was made clear that a separate DORA / ICT strategy would not be required, as long as the requirements were covered under existing or other strategies. This requirement could lead to competent authorities requiring a separate DORA strategy in contravention to the prevailing approach. For those institutions which do have a separate DORA strategy, there is no current requirement under DORA for links between it and the business strategy beyond the requirement that the institution be able to describe how the DORA strategy supports the business strategy. Such links may be more common in IT strategies. The supervisory expectation as currently drafted could be seen as moving the goalposts, and lead to a duplication of strategies which would increase the complexity of governance.

- Paragraph 197 states that, "Competent authorities should assess the materiality of operational risk arising from third-party service providers". This goes against the fundamental approach to both the assessment of third-party service providers, and established supervisory practice. Requiring competent authorities to independently assess the materiality of risks associated with third parties would be a significant operational demand on both competent authorities and institutions, and would likely lead to competent authorities coming to inaccurate conclusions. It would be more appropriate for competent authorities to assess the institution's approach to determining the materiality of operational risk arising from third-party service providers. The same paragraph provides that "when assessing third-party risk management, competent authorities should refer to the DORA framework for ICT services provided by ICT third-party service providers and the EBA Guidelines on the sound management of third-party risk for other third-party services". Such wording should be clarified to limit assessments to specific requirements under DORA on ICT risk management, and the EBA Guidelines on the sound management of third-party risk for other third-party services, rather than to include broad references to both frameworks.

- Paragraph 208 refers to competent authorities using reports of significant cyber threats as a source of information. We would emphasise that the reporting of significant cyber threats is on a voluntary basis under DORA, and may not be available to all competent authorities. We would welcome the EBA clarifying that this may be a source of information where available.

- Paragraph 216.i. states that competent authorities should review the institution's level of adoption and integration of digital technologies. Digital technologies is not a clearly defined term, and could refer to anything from the use of digital calculators to the deployment of sophisticated AI. Furthermore, a general expectation that the competent authorities review institutions' use of digital technologies, without links to a specific desired outcome, risks overstepping the boundary of supervisory responsibility into taking a direct hand in institutions' IT strategy.

- Paragraph 216.o. requires competent authorities to review institutions' vulnerabilities, however it does not define what sort of vulnerabilities this refers to. For example, software vulnerabilities are usually normally very point-in-time, and often resolved quickly after they are identified. As such, the specific vulnerabilities which might exist at the time of the supervisory review and evaluation process ("**SREP**") are unlikely to be representative of the steady state. Furthermore, the sharing of vulnerabilities outside of the institution can pose a material security risk to institutions, as any sharing of this information increases the likelihood that these vulnerabilities will become known to bad actors. We would propose that instead, competent authorities should consider the institution's approach to identifying the external threat environment, rather than seek to identify the threats and vulnerabilities themselves.

  Paragraph 217 states that competent authorities should "form an opinion on which ICT systems and ICT services support critical or important functions". In line with our other comments, this runs counter to established supervisory processes and the risk-based approach in DORA. Under DORA Article 5, financial entities are responsible for identifying their critical or important functions and the supporting ICT systems to ensure "effective and prudent management of ICT risk". Supervisors should assess the adequacy of the institution's methodology and governance for making these determinations, not substitute their own assessment. It would be more appropriate for competent authorities to review the approach that institutions have taken to determining which ICT systems and ICT services support their critical or important functions.

- The title, "Identification and mapping of material ICT risks to critical ICT systems and ICT services" on page 89 uses terminology which is not present in the existing regulatory framework. Rather than referring to critical ICT systems and ICT services, we would propose that this be amended to "ICT systems and ICT services supporting critical or important functions".

- Paragraph 218 states that competent authorities should "form an opinion on the material ICT risks that can have a significant prudential impact on the institution's ICT systems and services that support critical or important functions". This expectation appears to shift primary responsibility for ICT risk identification from the institution to the competent authority, which is inconsistent with the first-line responsibility model established under DORA. Similarly to our other comments, it would be more appropriate for the competent authorities to review the institution's approach for determining the material ICT risks to which they are exposed.

  Paragraphs 227 states that "competent authorities should assess whether the institution has established effective business continuity management with tested business continuity, response and recovery plans covering at least its critical or important functions, including those contracted to third-party providers", and paragraph 229.e. states that "competent authorities should assess whether the institution's business continuity, response and recovery plans [involve] the institution's third-party service providers where possible". The wording of both sections should be clarified and linked to specific DORA requirements or obligations, making sure it does not extend or broaden further DORA requirements. DORA requires for institutions to maintain their own business continuity plans when using third-party service providers and requires such third-parties to maintain their own independent resilience frameworks.

- Paragraph 232.c. does not recognise that the management body may delegate some of its responsibilities for follow-up and response to audit findings, nor does it consider the materiality of audit findings in question. We would propose that this be amended to read, “adequate follow-up and response by the management body or its delegates on material ICT related audit findings and findings reported under Article 13(5) of DORA”.

- Paragraph 233.a. requires competent authorities to assess "the adequacy of institution's ICT risk management policies, processes and procedures." The term "adequacy" is subjective and undefined, which may result in competent authorities taking divergent views on what constitutes adequate ICT risk management, leading to institutions required to request contractual changes from third-party service providers in exceeds of DORA's obligations, going against DORA’s fundamental driver of offering consistency in supervisory expectations across member states. We recommend removing the term " adequacy". The same concern applies to paragraphs 233.b., c., d., and g.

- Paragraph 245 refers to monitoring of the maturity level of an institution’s operational resilience. Maturity isn’t clearly defined in this context, and there is a risk that this could decouple the expectations from the degree of risk faced by the institution. An institution’s approach to resilience should be proportionate to the risks to which it is exposed. As such, we would propose that the wording be updated to instead refer to the effectiveness or the appropriateness of the institution’s operational resilience.

  Moreover, the SREP Guidelines would apply to the EU banking sector-only, creating operational resilience supervision to a facet of the EU financial sector, and leaving insurance, pensions, capital markets, asset management, asset management, financial market infrastructures, credit rating agencies, benchmarks or crypto-asset providers subject to different obligations. This would go against the aim of harmonisation introduced by DORA and applicable to the entire financial sector.

  SREP Identification of Material ICT Risk Assessment
  The SREP outlines how competent authorities should review an institution’s ICT risk to create an ICT risk profile for each institution and determine their inherent ICT risk. The factors competent authorities should consider in 216(a-o) include a significant range in terms of their impact on the ICT risk of a financial institution, which could both vary deeply across each institution or be highly subjective to each competent authority. For instance, (i) states that a financial institution’s “adoption and integration of digital technologies” should be considered. An institution could have highly effective controls in place and utilize digital technologies that provide a higher degree of resilience than former legacy systems. The opposite could be true as well. Moreover, the same level of subjectivity could be applied to (b), (c), (e), (g), (h), (m), (n) and (o). Each factor could demonstrate an effective control culture or the exact opposite.

  Factor (f) includes the “recommendations and opinions of Lead Overseers (LO),” which would constitute the opinions of the LOs concerning the risk associated with Critical Third Party Providers (CTPPs). The risk associated with CTPPs, while important, do not consider the mitigating controls, commercial relationship or dependency one institution would have with that CTPP. An institution’s inherent ICT risk influences their SREP scores and has a direct impact on their supervision, therefore FIA encourages greater considerations of the factors a competent authority should take into account and provide a greater level of detail regarding why those factors relate to risk.

Consistent and Proportionate Application of SREP to Institutions

Directive 2013/36/EU requires competent authorities to establish the frequency and intensity of their SREP and take "into account the principle of proportionality" (Article 97), while the EBA is required to ensure there is consistency in the SREP (Article 107). Institutions often find the SREP opaque and it is unclear how the instruments available to competent authorities interact with SREP scores or how competent authorities maintain proportional SREP. The industry would welcome a greater level of transparency from competent authorities and the ability to engage more collaboratively regarding interpretations of requests for information ("**RFI**") or instrument outcomes.

The following measures demonstrate an overly burdensome and duplicative SREP:

- **Structure of Supervisory Instruments:** Competent authorities are able to utilize an array of supervisory instruments to inform their SREP and determine the ICT risk for an institution. The number of instruments available to authorities have increased, however, it is unclear how these instruments feed into each other, lead to the SREP score, and how they are chosen throughout a year. The ECB is able to force an institution to submit an Information Technology Risk Questionnaire ("**ITRQ**"), a DORA Risk Management Framework ("**RMF**") Review and face a substantive RFI via a deep dive or a targeted review request. This could include a further on-site inspection, a DORA threat-led penetration test and participation in a cyber stress test. A competent authority is required to ensure that the SREP is proportionate to the risk for the institution and, while there are numerous instruments available, they should not all be utilized throughout a single year. Institutions, in addition, do not have transparency concerning how each instrument respectively influences their SREP score and would welcome more transparency concerning their role in a competent authority risk assessment.

- **DORA Risk Management Framework (RMF) Review & ECB Information Technology Risk Questionnaire (ITRQ):** The ECB requires directly supervised institutions to submit the ITRQ under the SREP. The ITRQ is an extensive RFI, covering over 300 separate ICT Guideline-related RFIs covering the entire IT infrastructure of the institution. Approximately 100 RFIs in the ITRQ focus on the institution's compliance with DORA. The DORA RMF Review, alongside, is a 40-50 pages overview of a institution's compliance with the risk management framework requirements in DORA. Both reports are excessively duplicative and do not reflect a proportionate or consistent application of the SREP for ECB-supervised institutions. Directive 2013/36/EU requires competent authorities to consider their SREP annually and FIA encourages a rationalization of RFIs by the ECB to reflect an institution's compliance with DORA.

- **Dual ITRQ Requests:** The ECB has requested two ITRQs in 2026 due to the outcomes of EBA's SREP reform, with each ITRQ covering 6-month periods. The end-of-year timelines for ITRQ requests allowed institutions to provide end-of-year financial and HR-related information, as this aligned with annual reports and accounting with institutions. Requesting mid-year ITRQs creates substantial issues regarding the ability for institutions to collect information that is not within the accounting cycle. Equally, following the consultation on the SREP Guidelines, it is unclear why a further ITRQ is required, with the ICT Guidelines broadly following the previous Guidelines and DORA RFIs (over 100) already being included within the first ITRQ. Having two ITRQs is disproportional and supervised institutions request further clarification why they are required.

- **Industry Consultation:** More aspects of the SREP should be open for industry consultation. While the SREP Guidelines provide transparency regarding considerations for risk, they do not account for how SREPs are operationalized by competent authorities. RFIs, ITRQs, CSTs all could benefit from increased input from the industry and the use of cybersecurity expertise within institutions to increase their effectiveness. Institutions would welcome an additional level of engagement before SREP scores are provided and the ability to speak to Joint Supervisory Teams if there are aspects of misinterpretation. Institutions are often caught unaware of risks expressed within supervisory letters and could have been engaged or remediated earlier.

Quantification of ICT Risk

The SREP Guidelines place a significant degree of importance on the quantification of ICT risk and the utilization of an institution's reporting metrics, without adequate consideration of the quality of risk management practices or the effectiveness of controls. FIA recommends that greater consideration is given to the other SREP instruments available to competent authorities and that the experience of supervision is directly inputted into the risk score of an institution. An over-reliance on internal reporting metrics, or quantification, directly correlates to a higher risk score to larger institutions with strong reporting cultures. More conservative institutions, who may identify a higher number of ICT risks, choose lower impact tolerance levels or report more frequently, would be penalized as having higher inherent risk. The SREP Guidelines therefore directly discourage accurate metrics through justified expectations of higher levels of supervision.

For instance, the following metrics included are stated as directly influencing ICT risk, despite the counter fact that high metrics relate to a strong cybersecurity culture within an institution with a stronger understanding of its ICT risk or controls:

- DORA operational incident reports: Incident reporting does not reflect the controls environment, risk posture or profile of an institution. A payments institution, who is highly likely to report more frequently due to geographical spread and economic impact criteria, will be disproportionately viewed as higher risk in comparison to a jurisdiction-specific retail bank.

- Reporting to management bodies: The severity level or frequency of reporting to management bodies will vary according to each institution and could be reflective of both higher ICT risk or an effective cybersecurity controls culture.

Concentration Risk

We note the emphasis placed by the SREP Guidelines on subcontracting chain length and complexity as drivers of concentration risk within the inherent operational risk assessment, without establishing objective criteria or thresholds for assessment. Institutions must have visibility of their full subcontracting chain in order to appropriately mitigate risks. However, whilst we recognise that complex or layered subcontracting arrangements can, in practice, make it more difficult for institutions and competent authorities to identify, monitor and manage underlying dependencies, length and complexity of the supply chain, in themselves, are not determinative of concentration risk. Concentration risk is driven by a range of factors such as the level and criticality of exposure, substitutability, and the degree of reliance on a limited set of providers. We would therefore welcome clarification that subcontracting chain complexity should be considered by competent authorities as an important but contextual factor based on the institution's risk management approach and

mitigation measures, rather than a standalone proxy for concentration risk. The SREP Guidelines should provide objective criteria for assessing concentration by competent authorities.

Given the clear and increasing supervisory focus on concentration risk, we consider it important that institutions are provided with greater transparency and clarity on the supervisory approach to assessing concentration risk in practice, including how subcontracting complexity is weighed alongside these other factors. This would enable institutions to better align their risk management approaches with supervisory expectations.

Subsidiary Considerations in the SREP

The SREP Guidelines state that competent authorities should "assign different categories to subsidiaries" (11a) and include one consideration of subsidiaries within the internal governance guidance. This does not adequately reflect ICT risk or how effective cybersecurity risk management occurs across cross border institutions. FIA recommends that further consideration is given to the idiosyncrasy and effective cyber risk management that are inherent to a subsidiary or an institution that operates across multiple jurisdictions. Best practice in cybersecurity risk management is to maintain a level of centralized control over policies, frameworks and controls that are consistent across all entities. The parent company, or headquarter, will pool a level of expertise, due to the technical nature of cybersecurity and the ability to provide the highest level of expertise across all entities. Incident response, incident recovery and crisis management all benefit from centralized expertise and structures that allow for rapid coordination.

Subsidiaries retain autonomy to implement additional controls and governance structures to comply with regulatory requirements. Cybersecurity risk management does not constitute the same form of risk as prudential or capital requirements (i.e. capital flight concerns or capitalization of the individual entity) – enforced subsidiarization of all forms of cybersecurity risk management would remove the benefits to elements of centralization and increase the level of risk to the subsidiarized entity. The ICT Guidelines and the SREP scores do not sufficiently reflect best practices for subsidiaries or cross border institutions and need to develop a more nuanced perspective concerning the inherent risk or effective cybersecurity controls. Inherent risk score should not be de facto unimprovable due to perceived risk associated with being a subsidiary.

Limitation of third-party arrangements for critical or important functions

Under Table 11 on potential and non-exhaustive list of supervisory measures stemming from the assessment of operational risk and operational resilience, the DORA framework under article 50 covers competent authorities' supervisory powers, and the SREP Guidelines should not extend this further or include explicit rights not included under DORA.

Assessment of ICT Risk Management Framework

Paragraph 232 in the assessment of an institution's ICT risk management framework states that the institution should have assigned the responsibility of "managing and overseeing" ICT risk to an independent control function. An independent function cannot "manage" ICT risk and this should be undertaken by the first line of defense. In this respect, we strongly encourage the word "manage" is removed as this is not reflective of the role of an independent control function.

ICT Audit Findings to be timely verified, remediated and formally followed up

Paragraph 235 requires that "critical ICT audit findings are timely verified and remediated" and that "ICT audit findings, including agreed actions, are formally followed up." While institutions must maintain robust audit processes, this language may be interpreted as indirectly extending audit verification and audit remediation obligations further than what is already included in DORA. Furthermore, audit findings reflect the institution's specific risk assessment, which may not align with the third party's risk management approach.

We recommend clarifying that paragraph 235 applies to the institution's own remediation processes and governance, and that competent authorities should assess whether institutions have appropriate processes for reviewing audit findings including with third-party service providers, when applicable.

Third-country branches

Paragraph 518 requires for third-country branches to have "access to all information required to exercise its monitoring including when using subcontractors". The wording should be amended to avoid overly broad interpretations by limiting the scope to information the head undertaking has access to and that is necessary for the third-country branch to exercise its monitoring obligations, including when subcontractors are used.