DORA - Draft RTS (Second Batch)

Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions, as mandated by Article 30(5)

March 2024

Executive Summary

AFME welcomes the opportunity to respond to the draft Regulatory Technical Standards (RTS) specifying elements which a financial entity needs to determine and assess when subcontracting. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Our response to this consultation is from the perspective of our bank members, focusing on those issues which are most relevant to wholesale capital markets. We are responding to each of the specific questions set out in the consultation paper, but wanted to raise the following overarching points:

1. **The obligations on financial entities will not be practical without a robustly proportionate and risk-based approach, limiting the scope to *material subcontractors* who effectively underpin critical and important functions.**

   The proposal for financial entities to monitor the entire supply chain, without the application of a materiality threshold, is both lacking in practicality and proportionality. The current expectation would:

   - Add significant complexity to a financial entity's (FE's) risk management practices.
   - Divert risk management resources away from focusing on where the real risk lies.
   - Goes beyond paragraph 80 of the existing EBA Outsourcing Guidelines which focuses on *subcontracting that could have material adverse effects on the provision of a critical and important function or would lead to a material increase in risk*.
   - Create misalignment with the register of information which focuses on subcontractors who *effectively underpin* ICT services supporting critical and important functions.
   - Lack consistency with the risk-based and proportionate nature of the FSB Third-Party Risk Management Toolkit (Section 3.5)

   We welcome recent verbal assurances by the ESAs that financial entities should be focusing on those subcontractors who "*effectively underpin*" the services supporting Critical or Important Functions (CIFs). We recommend the definition of 'material subcontractors' in the register of information implementing technical standard (ITS) be ported into the final draft of this RTS. This alignment would be essential for the consistent approach to and application of the Level 1 and Level 2 third-party risk management requirements. AFME would also welcome an express confirmation by the ESAs that the RTS should be interpreted in a manner consistent with this existing FSB guidance.

   Additionally, we would call for the proportionality principle to be embedded throughout the RTS, for example by stipulating that information be gathered "if relevant". We are strongly of

the opinion this would help bolster consistency across the ESAs in their approach to the Level 2 instruments.

2. **Direct oversight of subcontractors by financial entities is not a necessary or appropriate regulatory measure.**

The draft RTS would in several instances leave the financial entity in the role of supervisor, for example tasked with verifying the contractual assurances of the subcontractor to the third-party provider. This is both inappropriate and lacking in practicality and reflects a step-change in proposed due diligence and oversight practices that may not provide any meaningful risk-management benefit and is not practicable. Direct oversight of subcontractors can be resource-intensive, diverting attention and resources from strategic risk mitigation efforts of both FEs and third-party providers. We advocate for a balanced and outcomes-based approach that allows FEs, while remaining ultimately accountable, to effectively manage material supply chain risks by leveraging their contractual frameworks with third-party providers, with flow-down guarantees addressing subcontracting arrangements.

3. **The application will risk operational stability if supervisors do not permit a phased, risk-based approach to contractual remediation, including a prioritisation of arrangements for 17th January 2025 and timeline for wider roll-out.**

We are mindful that the draft RTS on subcontracting builds on the Policy for ICT services, which specifies how financial entities must additionally review the provisions within contractual arrangements with third-party providers. Collectively these requirements could capture thousands of arrangements per firm and affect global framework agreements. Remediating the entirety by the implementation deadline is not feasible and could lead to financial entities terminating arrangements where this is no underlying rationale for doing so or lead to providers and subcontractors deciding to withdraw from the financial services market. Such unintended consequences could ultimately see DORA adversely impacting operational resilience, an outcome which would be regrettably counter-intuitive to the overall purpose of DORA. We call on the authorities to formally give assurances to industry that enforcement will permit a phased, risk-based approach, with firms able to prioritise those arrangements which have the greatest potential impact and provide a timeline for the wider roll-out to less critical services.

4. **The incoming Critical Third-Party Provider (CTPP) regime will see duplication in terms of oversight and information gathering. Authorities should in future leverage the CTPP databases on subcontracting.**

The requirements on CTPPs under DORA will inevitably lead to dual indirect oversight of subcontractors and duplication in terms of supply chain information gathering, on one hand by the financial entities themselves and on the other hand, the designated CTPPs. As we have urged in our response to the consultations on supervisory cooperation and oversight harmonisation, authorities should be using the same datasets where possible. Given their closer proximity with subcontractors, it is strongly advisable that financial authorities directly rely on the information captured by the CTPP Lead Overseers where possible.

Please see below our responses on questions 1 – 5. We remain available to discuss any further points raised.

Consultation Questions

Question 1 **Are articles 1 and 2 [Complexity and Risk Considerations and Group Application] appropriate and sufficiently clear?**

- We propose aligning Article 1 with the regulatory intention expressed in the background and rationale section, namely: "*While these RTS set out requirements regarding subcontracting by ICT third-party service providers for the use of ICT services supporting critical or important functions or material parts thereof, Regulation (EU) 2022/2554 also sets out risk management requirements for the use of ICT third-party services providers including subcontractors providing ICT services supporting functions that are not considered critical or important*". We would recommend to amend Article 1 as follows:

Current wording	Proposed wording
For the purpose of applying Articles 2 to 7 regarding the contractual arrangements between financial entities and ICT third-party service providers on the use of subcontracted ICT services and the conditions applying to it,	For the purpose of applying Articles 2 to 7 regarding the contractual arrangements between financial entities and ICT third-party service providers on the use of subcontracted ICT services ***supporting critical or important functions or material parts thereof*** and the conditions applying to it,

- As a point of principle, we note that the use of subcontractors could be deemed to lower the overall concentration risk if this diversifies the provision of services away from the third-party alone. Article 1, subparagraphs 1(b) and 1(i), appear duplicative in seeking to tackle the risks associated with concentration risk.

- Article 1, subparagraphs 1(f) – 1(h) do not appear relevant considerations when assessing the risks associated with subcontractors. Rather, these considerations are linked to the inherent risk level of the financial entities' planned usage of the service provided by the third-party provider. We therefore recommend removing these elements as they are already captured in the DORA policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions, as outlined in Article 1(h) – 1(j) of the RTS. If the ESAs are anticipating additional measures, for example specific scenario or stress testing under point (g) or any further analysis of concentration risk under point (i), we recommend this is clarified.

- AFME also flags that the requirement for financial entities and groups to re-engineer their existing third-party risk management systems around ICT providers, as a specific subset, entails a significant resourcing challenge. This is notwithstanding our assumption that the requirements do not capture non-EU subsidiaries contracting with non-EU providers.

Question 2 **Is article 3 [Risk Assessment regarding use of subcontractors] appropriate and sufficiently clear?**

- The proposed list of elements to be considered as part of the risk assessment is noted to be a non-exhaustive, yet comprehensive and mandatory list of considerations. We recommend

this is adjusted, with the principle of proportionality applied, to clearly indicate that the list includes factors to be considered by financial entities "subject to a risk-based approach". Additionally, without the explicit application of materiality, a number of the requirements would apply to an unnecessarily broad scope of subcontractors. These risks undermining the effective and efficient management of supply chain risks that have the potential to materially impact the delivery of the contracted service, or that pose a threat to financial stability. The volume of 4th party providers (in particular in the case of big tech vendors) would also entail a huge investment in effort, time and budget from the financial entities to evaluate each as proposed.

- In general, when assessing whether a third-party provider may use subcontracting, the FE will review the provider's approach to oversight of their subcontractors and will include obligations in the contractual agreement between the FE and the third-party provider requiring the FE's consent for subcontracting, setting out requirements for the management of those subcontractors and the level of service expected. This may include right to attend the third-party provider's audit of the subcontractor as it pertains to the FE's services. This places the obligation for ensuring appropriate contractual provision between the third-party provider and the subcontractor, and for the oversight of subcontractors with the third-party provider. A financial entities' third-party risk management program is the most effective way of ensuring risk management practices and regulatory obligations cascade down the supply chain and that third parties and their subcontractors are held to established standards, whilst the FE remains ultimately accountable for assessing the associated risks and compliance with its own regulatory obligations. Financial entities implement comprehensive, risk-based due diligence processes and supplier controls to ensure the risks associated with the use of subcontractors are effectively managed and mitigated. These measures are upheld, and are enforceable, through the contractual framework between the financial entity and its third-party and typically include the following:

    - Third-party providers must seek approval or consent before engaging a 'material' subcontractor. A materiality threshold is applied to this requirement so that financial entities and third-party providers can focus on managing only those suppliers which present a risk to the delivery of the service.

    - Third-party providers are required to due diligence their subcontractors and to make the results of this due diligence available to the FE upon request. This obligation typically applies to any subcontractor, regardless of tier, that is 'material' to the delivery of the service. The ability to access due diligence materials is an important tool for providing visibility into a FEs risk posture (as it feeds into the risk assessment) and contractual flow down.

    - Third-party providers are contractually obligated to flow down their risk management and oversight obligations to the entire supply chain and, typically, audit rights are specified as needing to be flowed down to subcontractors.

    - Third-party providers are required to stand behind the performance of their subcontractors.

- It is an essential feature of the risk management and contractual framework that FEs leverage third parties as they are better positioned to manage and monitor their subcontractors effectively based on (i) their expertise and nuanced understanding of their service, the subcontractor and their control environments, and (ii) their direct contractual relationship with the subcontractor which can be effectively leveraged to enforce the risk management measures that flow down from the direct relationship between the FE and third-party. In the absence of a direct contractual relationship, it is not practicable for an FE to exercise direct oversight over subcontractors. This does *not* equate to the delegation of a FEs responsibility to manage subcontractor risk along the supply chain, but rather is critical to enabling strategic and effective risk mitigation practices. We advocate for a balanced and outcomes-based approach that allows FEs to effectively manage material supply chain risks, leverage contractual frameworks and third-party expertise, whilst remaining ultimately accountable to assess and monitor the risks associated with the ICT subcontracting chain, and their compliance with their own legislative and regulatory obligations. This accountability can be effectively managed through due diligence, audits, reporting mechanisms and assurance frameworks that ensure compliance with regulatory obligations.

- Requiring FEs to directly govern the contractual arrangements between the third-party provider and its subcontractors, or requiring FEs to provide direct oversight or management of the subcontractors will jeopardise this clear obligation and could undermine the legal protections that FEs currently benefit from, as well as complicating the flow of obligation from the subcontractor to the third-party provider and then to the FE. One example of how this uncertainty could arise is, if during the verification process, a subcontractor provides its assurances directly to the financial entity in writing, this might inadvertently create a collateral contract directly between the financial entity and the subcontractor. Additionally, contractual negotiations are usually highly commercially sensitive, and there may be confidentiality restrictions on sharing proposed contractual terms with a third-party (e.g. the FE). As such, we would strongly encourage the ESAs to avoid placing obligations on FEs to step in to this relationship, and instead leverage the well-established approaches leveraging a chain of obligations and oversight, which deliver robust results in an efficient manner.

- Due to the above, we object to those provisions which would see the financial entity stepping directly in between the third-party provider and subcontractor and acting as quasi supervisor. Key examples are:

    - Under Article 3(a), the due diligence processes implemented by the ICT third-party service provider is expected to be assessed by the financial entity *"(…) including by participating in operational reporting and operational testing as required by the financial entity".*

    - Article 3(1)(b) where ICT third-party providers are not just to inform financial entities of decision making relating to subcontracting, but to "involve the financial entity" in that decision making process. This is not appropriate, nor reflective of commercial practice. The "involvement" of a customer (in this case the FE) in the provider's decision-making process would be extremely complex, especially if the provider

supports CIFs for multiple FEs. There is a high likelihood that FEs' viewpoints on subcontracting could differ, and ensuring complete alignment between varying FEs as part of the decision making could prove prohibitively time-consuming, expensive and complex. This complexity and cost could lead to either third-party providers not being able to leverage the best subcontractors available for a given process, or even lead to them ceasing to offer services to FEs. Ultimately third-party providers are best placed to evaluate and implement remedial actions.

- Article 3(1)(e) where the FE is expected to ensure its risk management framework extends to monitoring and overseeing subcontractors *directly* where possible and appropriate. This is not an appropriate regulatory measure and lacks a clear and explicit application of proportionality. While FEs already monitor and oversee ICT services which have been outsourced, it would be extremely difficult and resource intensive to oversee subcontractors *directly* and would also compromise the obligation of the ICT third-party provider to oversee their subcontractors themselves. Firms will review their ICT providers' oversight of their subcontractors, and establish such responsibilities with the third-party providers directly, following which it is the provider's responsibility to oversee their subcontractors. In addition, multiple FEs may be using an ICT third-party provider. In such a situation there could arise circumstances in which multiple FEs are trying to oversee a given subcontractor in parallel, which could give rise to conflicting demands and could even compromise the integrity of the service.

- Additionally, the reference to step-in rights as part of the risk assessment under Article 3(1)(f) has caused confusion. For the sake of clarity, we suggest this reference is removed from the risk assessment, with step-in rights addressed separately in line with current operational practice.

- We would therefore suggest the change below:

Current wording	Proposed wording
a) that the due diligence processes implemented by the ICT third-party service provider ensure that it is able to select and assess the abilities, both operational and financial, of prospective ICT subcontractors to provide the ICT services supporting critical or important functions, including by participating in operational reporting and operational testing as required by the financial entity;	a) that the due diligence processes implemented by the ICT third-party service provider ensure that it is able to select and assess the abilities, both operational and financial, of prospective ICT subcontractors to provide the ICT services supporting critical or important functions, ~~including by participating in operational reporting and operational testing as required by the financial entity~~;
b) that the ICT third-party service provider will be able to inform and involve the financial entity in the	b) that the ICT third-party service provider will be able to inform ~~and involve~~ the financial entity of its

decision-making related to subcontracting when relevant and appropriate;	decision-making related to subcontractors when relevant and appropriate;
e) that the financial entity has adequate abilities, expertise, financial, human and technical resources, applies appropriate information security standards, and has an appropriate organisational structure, including risk management, incident response and business continuity management and internal controls, to monitor and oversee the ICT service that has been subcontracted or, where possible and appropriate, the subcontractors directly;	e) that the financial entity has adequate abilities, expertise, financial, human and technical resources, applies appropriate information security standards, and has an appropriate organisational structure, including risk management, incident response and business continuity management and internal controls, to monitor and oversee the ICT service that has been subcontracted ~~or, where possible and appropriate, the subcontractors directly~~;
f) the impact of a possible failure of a subcontractor on the provision of ICT services supporting critical or important functions on the financial entity's digital operational resilience and financial soundness, including step-in rights;	f) the impact **that** a possible failure of a subcontractor **could have** on the provision of ICT services supporting critical or important functions **and, consequently,** on the financial entity's digital operational resilience and financial soundness~~, including step-in risks rights;~~

- Of particular concern is the further requirement under Article 3(1)(c), for financial entities to impose and assess specific clauses within the contracts of the third-party provider and subcontractor which does not appear consistent with long standing legal principles over contract confidentiality, given copies of subcontracts would not typically be made available. Nor does the assertion that such an approach can ensure a financial entity is able to comply with its own obligations, appear realistic or fool-proof. As such, not only does this requirement risk overstepping the legal boundaries set for contractual relationships but making a FE's compliance with its own obligations contingent upon the FE assessing that certain terms have been replicated, risks undermining the FEs own ability to fulfil its regulatory obligations. In addition, the requirement to replicate contractual clauses may cause undue legal complexity in some contractual arrangements, in particular if a subcontractor is supporting multiple FEs, all of which may have different drafting for their contractual clauses. The focus should be on ensuring that the contractual framework between the FE and its third-party is robust and provides for the flow down of obligations and standards to material subcontractors and the replication of certain clauses in downstream agreements. This would reach the same intended outcome, whilst remaining in line with accepted contractual principles and frameworks. It also appears that any attempt to impose new contractual provisions beyond those already set out in DORA Article 30(2) and 30(3), goes beyond the

mandate for this RTS as set out in DORA Article 30(5). We therefore recommend that this requirement is removed.

- Finally, we:
    - Flag the draft does not address how open-source solutions, which are often developed and maintained by a community rather than a single third-party service provider, would fit into the subcontracting framework.
    - Assume that the obligation on auditing under Article 3(1)(i) relates only to the third-party provider in the case of the financial entity, and that any further auditing of subcontractors lies with the relevant third-party providers as appropriate.

Question 3 **Is article 4 [Description and conditions for subcontracting] appropriate and sufficiently clear?**

- As proposed, Article 4 will amount to a significant uplift in compliance burden for financial entities, despite the fact the risks within scope are largely captured in existing operational practices. In particular we flag:
    - The fact that each ICT service eligible for subcontracting must specify all of the listed criteria, regardless of whether subcontracting actually occurs, and irrespective of how such services are often bundled within framework agreements.
    - The obligation to reverse engineer these existing operational practices into contractual provisions relevant for the financial entity. This can be seen for example under Article 4(g) with the requirement to incorporate within contractual arrangements incident response and business continuity plans, which are typically separate operational documents, as recognised in the corresponding provisions of the EBA Outsourcing Guidelines (para 75 g, i & l). Similarly, the requirement to include in the contractual arrangement, under Article 4(1)(d), information on the location and ownership of data processed and stored. Typically, this would be maintained in systems of record rather than within the actual contract, which will then have to be continuously updated every time a new or changed subcontractor relationship is communicated. The term "ownership of data" in Article 4(d) may also lead to interpretation issues given the legal concept of "data ownership" may not exist in the law of some member states. We suggest that the wording "ownership" be replaced by "processed or hosted on behalf of the financial entity" for the sake of clarity.
- Additionally, we highlight that:
    - Article 4(1)(b) does not seem relevant to an RTS on subcontracting, given it relates to the relationship between financial entity and third-party provider. This is illustrated by the duplication of this requirement within Article 30(3)(b) of DORA. We recommend this clause is removed.

- Article 4(1)(c) is lacking in practicality/proportionality in explicitly seeking an assessment on "all" risks associated with the location of a potential subcontractor. We encourage alignment with 78.c and 75.f of the EBA Guidelines. Article 4(1)(j) is likewise lacking in proportionality by failing to stipulate such termination rights relate only to material breaches, in line with Section 13.4 of the EBA Outsourcing Guidelines. We recommend:

Current wording	Proposed wording
c) that the ICT third-party service provider shall assess all risks including ICT risks, associated with the location of the potential subcontractor and its parent company and the location where the ICT service is provided from;	c) that the ICT third-party service provider shall assess **relevant** ~~all~~ risks, including ICT risks, associated with the location of the potential subcontractor and its parent company and the location where the ICT service is provided from;
j) that the financial entity has termination rights in accordance with article 7, or in case the provision of services fails to meet service levels agreed by the financial entity.;	j) that the financial entity has termination rights in accordance with article 7, or in case **of material breach** of the ~~provision of services fails to meet~~ service levels agreed by the financial entity.;

- Article 4(e) requires FEs to include in their contractual terms with third parties the need for the third-party provider to "specify the monitoring and reporting obligations of the subcontractor…where relevant, to the financial entity". Given that third-party providers will have clear monitoring and reporting obligations towards FEs, a more practical approach is to ensure that subcontractors conduct the appropriate monitoring and reporting towards the provider, which will in turn monitor its services supported by the subcontractor, and report as appropriate to the FE. We would propose removing from the text, "and where relevant, towards the financial entity":

Current wording	**Proposed wording**
e) that the ICT third-party service provider is required to specify the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, and where relevant, towards the financial entity;	e) that the ICT third-party service provider is required to specify the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, ~~and where relevant, towards the financial entity~~

- Article 4(1)(f) requires FEs to include in their contractual terms with third parties the need for the third-party provider to "ensure the continuous provision of the ICT

services supporting critical or important functions…". This could imply that zero disruption can be contractually guaranteed, which runs counter to the underlying assumptions in DORA that operational disruption is unfortunately an inevitability. We recommend this clause is removed. Alternatively, that the ESAs emphasise the requirement of the third-party provider to periodically assess the resilience and recovery of these functions, including the case of a failure of a subcontractor.

Question 4 Is article 5 [monitoring of the supply chain] appropriate and sufficiently clear?

- As stated above, we view the proposed Article 5 to be lacking in proportionality and practicality. The explicit reference to the "entire ICT subcontracting chain" would capture a whole suite of subcontracting which has less to no relevance for the purposes of operational resilience given that not all ICT services supporting critical or important functions carry the same level of risk (or importance) to a financial entity; and accordingly not every subcontractor linked to an ICT service supporting a critical or important function is equally important in terms of potential impact. Neither does the expansive terminology reflect recent conversations on the need for financial entities to focus on those subcontracting arrangements which are effectively underpinning the services supporting CIFs. As recommended above, importing this definition would ensure that financial entities are able to take a risk-based approach to DORA compliance and focus efforts on those subcontracting arrangements which are likely to have a higher level of potential impact. This approach will also reflect the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management and could be bolstered by further operational guidance on the expected level of monitoring. We strongly urge the following:

Current wording	Proposed wording
Article 5 Monitoring of the entire ICT subcontracting chain by the FE 1) When an ICT service supporting critical or important functions is subcontracted the financial entity shall fully monitor the ICT subcontracting chain and shall document it, including on the basis of the information provided by the ICT third-party service provider, in accordance with Article 28 paragraphs (3) and (9) of Regulation (EU) 2022/2554.	Article 5 Monitoring ~~of the entire ICT subcontracting chain~~ by the FE **of material ICT subcontracting arrangements who are underpinning the delivery of critical and important functions** 1) When an ICT service supporting critical or important functions is subcontracted the financial entity shall ~~fully~~ monitor the **material ICT subcontracting arrangements** ~~subcontracting chain~~ **which are effectively underpinning the critical and important functions of the financial entity (i.e. to the extent such subcontracting could have material adverse effects on the provision of a critical and important function or would lead to a material increase of risk),** and shall document it**,** including **as appropriate** on the basis of the information provided by the ICT third-party service provider, in accordance with Article 28 paragraphs (3) and (9) of Regulation (EU) 2022/2554.

- We also strongly recommend the deletion of Article 5(2). The proposal for a financial entity to review the contractual documentation between third-party providers and subcontractors introduces significant legal, commercial, and operational complexity. It is likely to breach long standing legal principle and raises serious questions around who bears the burden of liability. Legally, it puts at risk the core tenet of confidentiality as between contracting parties and could raise conflict of law considerations, (if e.g. supplier pricing arrangements are exposed to their FE clients). It is also questionable how such monitoring could be achieved in the absence of a specific contractual arrangement between the financial entity and subcontractor. Regardless, operationally, the sheer volume of thousands of financial services firms intervening in contractual negotiations would impose a huge administrative burden, extend negotiation timelines and potentially create industry-wide disruption that itself would risk the stability of the financial system.

- At the very least, the ESAs should amend Article 5(2) to focus monitoring obligations solely on key performance indicators, in line with the EBA Guidelines on outsourcing (section 14). Specifically, we recommend:

Current wording	Proposed wording
(2) The financial entity shall monitor subcontracting conditions, including through the review of contractual documentation between ICT third-party service providers and subcontractors, as appropriate, and key performance indicators to ensure that all the conditions referred to in Article 4 are complied with along the entire ICT subcontracting chain	(2) The financial entity ~~shall~~ **has the right to** monitor subcontracting **arrangements,** ~~conditions~~, ~~including through the review of contractual documentation between ICT third-party service providers and subcontractors, as appropriate,~~ **operational dependencies,** and key performance indicators to ensure that all the conditions referred to in Article 4 are complied with **for those subcontractors which effectively underpin the financial entity's critical or important functions** ~~along the entire ICT subcontracting chain~~

Question 5 Are articles 6 and 7 [material changes and termination] appropriate and sufficiently clear?

- Members are largely comfortable with these articles, and the read-through to corresponding Level 1 provisions, provided they relate only to those services effectively underpinning CIFs, and we recommend this is explicitly referenced within Article 6(1). Several members have though called for additional guidance on what amounts to "material change", with all agreeing that failure to adopt proportionality would again create a lack of practicality, given the level of rotation of 4th party providers supporting a critical service which would make it almost impossible to continuously track each and every change in the subcontracting chain.

- We additionally recommend that the ESAs adhere more closely to the EBA outsourcing guidelines in determining whether the third-party provider had the consent of the financial entity to enact material changes with regards to subcontracting. The proposal as drafted gives the option of explicit consent or consent by silence, which could give rise to conflicting understandings. We recommend:

Current wording	Proposed wording
Art 6 (3) The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period.	3) The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has ~~either approved or~~ not objected to the changes by the end of the notice period**.**

- We also flag it is unnecessary for financial entities to provide the third-party provider with any risk assessment, but rather any preferred adjustments to the proposed material changes. Such an outcomes-based approach will assist in ensuring the process is as efficient as possible, and mitigate the incoming burden on third-party providers. We recommend:

Current wording	Proposed wording
2) The financial entity shall inform the ICT third-party service provider of its risk assessment results as referred to in paragraph 1) by the end of the notice period.	2) The financial entity shall inform the ICT third-party service provider of **any necessary adjustments or objections to the material changes** ~~its risk assessment results as referred to in paragraph 1)~~ by the end of the notice period. This would negate the need for a separate clause under Article 6(4).

Contacts

AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu
AFME	Stefano Mazzocchi	+32(0) 2883 5546	stefano.mazzocchi@afme.eu
AFME	Coen Ter Wal	+44(0)020 3828 2727	coen.terwal@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/