Banking & Payments Federation Ireland

BPFI Response to the Central Bank of Ireland Draft Cross-Industry Guidance on Outsourcing- CP 138

July 2021

www.bpfi.ie

General Comments:

Banking & Payments Federation Ireland (BPFI) is the voice of banking and payments in Ireland. Representing over 70 domestic and international member institutions, we mobilise the sector's collective resources and insights to deliver value and benefit to members, enabling them to build competitive sustainable businesses, which support customers, the economy and society.

BPFI welcomes the opportunity to respond to the Central Bank of Ireland (CBI) public consultation on the draft Cross Industry Guidance on Outsourcing (CP 138). (the **"Guidance")**

This consultation follows on from the publication of discussion paper on outsourcing in November 2018 by the Central Bank of Ireland (CBI) and the industry outsourcing conference in April 2019. Meanwhile the European Banking Authority has updated its guidelines on outsourcing which came into effect in September 2019, where banks have until December 2021 to update all existing documentation to meet the standards which address a wide range of issues. Many member banks, and particularly international banks operating in Ireland, have started making necessary changes at a group level to be implemented in each European jurisdiction following the EBA guidelines. We note that, and detail in this submission, some of the requirements proposed in this consultation are in addition to wider European requirements set out by the EBA, which adds extra layer of complexity for group wide policy implementation as certain aspects of implementation will differ in Ireland compared to other group operations. BPFI members would like further clarity and guidance from the CBI as to the reasons why these additional requirements are needed and whether the CBI perceives that the risks associated with outsourcing activities carried out by banks operating in Ireland are higher than operations in other EU jurisdictions.

BPFI members would like further clarity and guidance from the CBI on the applicability and practical roll-out of the Guidance in respect of branches of international banks operating in Ireland and how such Guidance, being at Irish level, will impact such international banks in respect of their overall outsourcing policies and procedures.

BPFI members believe that a transitional period should be set out for any requirements that exceed those set out under existing sectoral legislation, regulations and guidance. Specifically, the Guidance sets out that for regulated firms who fall within scope of the EBA, EIOPA and ESMA Guidelines, implementation will be aligned with timelines for these Guidelines. A transition period should be permitted for the implementation of any additional requirements above what is set out under EBA. In addition, for all other firms we believe that the timeline is to be notified by an industry letter which should also consider similar implementation timeframes as was set out under EBA Guidelines.

Consultation Paper Sections

1. Assessment of Criticality or Importance of activity/service to be outsourced.

Point 1 (d) (iv) (page 12) refers to reviews of assessment of criticality or importance "if an organisational change at the OSP or a material sub-outsourced service provider takes place, including a change of ownership or to their financial position".

We believe that the definition of material sub-outsourcer/material sub-contractor is required along with clarity if "critical" or "important" is one single category and there is no difference between the two.

2. Intragroup Arrangements

The Guidance refers to at 2(d) (page 13), ensuring, "that the resolution of any potential conflicts of interest is provided for in the governance arrangements". We believe that the CBI could be more explicit here in detailing their expectations in particular for Less Significant Institutions' (LSIs) intragroup arrangements in resolving conflicts of interest i.e., there is no external bidding process and the internal option is the only option contemplated based on practical cost and centre of excellence considerations. The EBA guidelines state that in an intragroup context, arrangements should be at arm's length so perhaps the CBI can utilise similar language/methodology.

3. Outsourcing and Delegation

The Guidance states that in respect of the assessment of delegation arrangements, the CBI expects that regulated firms to take note that "delegation" and "outsourcing" are not considered by the CBI to be different concepts and to treat delegated arrangements to the same onerous due diligence, oversight and monitoring as for other outsourcing arrangements.

BPFI acknowledges the CBI's views in relation to the concept of delegation. We also note that the CBI considers that the obligations of regulated firms with regard to the use of delegates are well covered in the relevant sectoral legislation, regulations and guidance. We agree that appropriate governance and risk management measures need to be in place in respect of delegated arrangements and that these must function effectively. However, BPFI members are of the view that existing rules governing the delegation of activities covered in relevant sectoral legislation, regulations and guidance are

indeed functioning effectively and are more than sufficient to ensure that regulated firms can demonstrate that they have appropriate oversight of such delegation arrangements (e.g. UCITS Directive and the AIFMD). To the extent that delegation arrangements are required to adhere to the current proposed Guidance over and above those rules, this will create duplicate requirements and attempt to remedy risks that are already appropriately addressed.

Do delegated arrangements need to explicitly be called out as in scope and flag them accordingly? We note that "delegated arrangements" are not defined in the Appendix, although it is stated that regulated institutions need to treat delegated arrangements to the same onerous due diligence, oversight and monitoring as for other outsourcing arrangements. BPFI members would like to receive further clarity on this.

4. Governance

4.1 The Role of the board and senior management

The CBI expects that the board, senior management or management body of regulated firms have a documented outsourcing strategy in place which is aligned to the regulated entity's business, strategy, business model, risk appetite and risk management framework. In addition, it is also expected that the outsourcing strategy should be supported through appropriate policies, procedures, and controls. Existing outsourcing risk management frameworks should be updated to ensure expectations set out in this Guidance are appropriately considered and addressed. This suggests that outsourcing strategy is intended to be a separate document to the business strategy.

We suggest that proportionality should be applied in this regard. For larger institutions with complex outsourcing arrangements, a dedicated outsourcing strategy may be appropriate, however for smaller organisations that avail of intra-group arrangements with their parent company, either in the State, EEA or in a 3rd country embedding the outsourcing strategy into the overall business strategy is more appropriate.

The Guidance reserves a number of activities specifically for the Board such as review and approval of outsourcing policy by the Board. Further reference that any outsourcing committee should be directly accountable to the Board implies that the committee would be a direct sub-committee.

We want to understand the implications with regards to some of the activities if they can / cannot be delegated to a junior committee by the Board.

The Guidance refers to having a comprehensive outsourcing policy in place which should be reviewed and approved by the board annually. We believe that the wording on frequency should be changed to "regular review and approval" as per the EBA guidelines.

4.2 Strategy and Policy for Outsourcing

We note that the ESMA guidelines on cloud-outsourcing also requires a "cloud -outsourcing strategy". In this regard, we expect this to be part of an overall outsourcing strategy and as outlined above ultimately embedded in the business strategy for small LSIs, noting that outsourcing strategy is supported by outsourcing framework. The outsourcing framework within entities is an element of the Operational Risk Framework as part of the overarching Risk Management Framework.

The Guidance, on page 16, states that, regulated firms have a documented firm-wide Outsourcing Policy, which is reviewed and approved by the board at least annually. BPFI members believe that this should be changed to "regular review and approval" as per the EBA guidelines. BPFI members do not object to Board review of the policy in principle, but we believe that the Risk Committee review and approval should be sufficient, given that the Board is involved in the Business / Outsourcing Strategy setting.

The Guidance refers to the requirement for a documented exit strategy as part of the outsourcing policy. Many of the international LSIs' business model is to leverage services from the parent which include critical services relating to IT, information security and risk data. If there were on-going or significant failures in terms of the delivery of these services, this would be indicative of serious issues at the Group. Alternative service providers cannot be readily found to replace the parent. The cost would be prohibitive. Therefore, for these critical services the exit plan will de facto refer to the Recovery and/or Resolution Plan for the operations in Ireland.

The Guidance, on page 18, states that outsourcing policy should also address differences in the regulated entity's approach to governance and management of outsourcing of intra-group OSP versus external third party OSP. The CBI has previously stated that there should be no differentiation between the treatment of intra-group and external outsourcing. Can we take this statement to mean that the two approaches can be treated differently as there is a view that intra-group arrangements are inherently less risky than true third-party outsourcing? Many of the international LSIs' modus operandi / business model is to leverage services from the parent. Replicating activities in smaller entities in Ireland will make it extremely difficult to do business in Ireland and would hinder future growth. Risk

is mitigated through an appropriate governance and oversight model, where the expertise is in the Irish based institution to monitor the delivery of services in line with agreed metrics with the parent.

4.3 *Record keeping (Documentation Requirements - Register/s) No Comments*

4.4 *Outsourcing of risk management and Internal Control Function No Comments*

5. Outsourcing Risk Assessment & Management

The Guidance refers to "step-in risk" which is the risk that the regulated firm may need to step in to provide financial support to an OSP or to take over its business operations. Is there an expectation by the CBI that step-in risk will ever apply to intra-group arrangements?

5.1 *Sub-Outsourcing Risk*

The Guidance notes that the Regulated firm should not agree to sub outsourcing unless the sub-contractor agrees to provide the Regulated firm and the CBI the same contractual rights of access and audit as those granted to the primary OSP. We believe that further clarification is needed as to how this can be achieved. Is it expected that the Regulated firm and CBI is explicitly referenced in the sub-outsourcing contract? Further is it the expectation that the Regulated firm would review each sub outsourcing contract to ensure the subcontractor has agreed to the appropriate sections. What is the expectation of CBI for firms "to ensure at a minimum that the OSP oversees and manages the activities of the sub-outsourced service provider…" (p. 21, e))

5.2 Sensitive Data Risk

A data management strategy is unlikely to be defined by each legal entity of a group. Can the CBI clarify if a group approach is sufficient in this regard? In addition, current policies in the firms in this area would already meet the EBA guidelines.

5.3 *Data Security - Availability and Integrity*

The statement at Section 5.3, paragraph 1 (page 23), that data should be ringfenced offline is inaccurate. Creating an offline copy of data is one control for data integrity, but it has significant

limitations, including the inability to quickly restore data in the event of a major ICT-related incident. Firms are increasingly moving towards data immutability as the most advanced method available for ensuring data integrity while allowing for recovery within RTO. We recommend that reference to offline data ringfencing be removed.

The Guidelines, on page 23, list a series of controls for data in transit, rest and memory. While we recognise these controls, we do not believe that all controls listed are applicable at all times. For instance, (g) data segregation in a multi-tenant cloud environment, may not be applicable for certain data or applications, for example publicly available data. Equally, segregation does not guarantee the confidentiality, integrity or availability of data hosted in a public cloud environment. While a firm might choose to isolate its applications and data, we do not believe this specific control should be prescribed as it may limit the ability of firms to take advantage of the unique offerings available in the public cloud environment and therefore hurt its ability to innovate. We recommend that the final sentence in the second paragraph under section 5.3 *be changed from "including the following" to "such as the following".*

5.4 *Concentration* Risk

The CBI defines concentration risk as the probability of loss arising from lack of diversification of OSPs. We wish to emphasise that this probability is a factor of more than the concentration itself, but of the resilience of the OSP and the controls the financial institution has in place. This is particularly the case for cloud services under the shared responsibility model in which the financial institution remains accountable for all factors and responsible for a number of elements which contribute to the resilience of the service.

We also note the importance of recognising the difference between intragroup and external OSPs regarding concentration risk. While we recognise that a financial institution can still be concentrated in an intragroup OSP, the financial institution has several advantages in an intragroup context, for instance direct access to the OSP in the event of an incident and a guarantee of prioritisation for response and recovery. In addition, concentration risk is inevitable in business models for small institutions which leverage skills and services from the parent. Typically, the revenue base will not support duplicating the functionality in Ireland or diversifying to other true 3rd party service providers. Anything other than using economies of scale and Centre of Excellence (COE) Models render local Irish entities as unviable.

Finally, we note that item Section 5.4 (e) (vi) (page 25) asks firms to consider the contribution of an outsourcing to 'broader systemic concentration risk' for the sector. We do not believe this is in the power of financial institutions to do as they lack the information necessary to make this assessment. We note that this factor is not included in the EBA Outsourcing Guidelines, and that this point was specifically noted by the EBA in their commentary on page 108 of the Final Guidelines regarding paragraph 59.

5.5 *Offshoring Risk*

The Guidance sets out specific tasks to risk assess offshoring, including specific 'country' risks – i.e. physical climate risk, cultural or language issues and employment conditions in offshore jurisdictions. Regulated firms may, if appropriate, be restricted from offshoring activities, where for example, the ability of the CBI to supervise is either severely constrained or non-existent. Firms must also inform the CBI of circumstances where such issues (as outlined above) may arise before committing to any offshoring arrangements in respect of the outsourcing of critical or important functions or services. Firms must also inform, by way of notification to and engage in dialogue with the CBI in sufficient time to permit appropriate supervisory consideration of those risks.

Due to the detailed descriptions of offshoring risk considerations, firms may have to enhance their risk assessments as these are not all covered in the EBA guidelines (e.g., cultural or language issues, employment conditions in offshore jurisdictions). This will create the requirement for regulated legal entities in Ireland to create unique risk assessments over and above what is set out by the EBA. BPFI members strongly believe that this request should be aligned with the EBA in this respect.

Further, in respect of the offshoring restriction, we would recommend the CBI provide clarity on jurisdictions that are out of scope from being restricted based on current information sharing requirements. We would recommend that EU jurisdictions are excluded from this potential restriction.

6. Due Diligence

We note the inclusion of additional due diligence requirements over and above EBA Outsourcing GL and ESMA Cloud Outsourcing GL, in particular:

- Page 27, f) Capacity of the OSP to keep pace with innovation within the market sector".

We would query the practicalities of risk assessing future innovation and would question the need for this additional information and request alignment to EBA Outsourcing GL instead. In addition, if the firm outsourcing the service require that additional services should match market pace, this would be agreed between the parties.

- Page 28, Section 6 paragraph 1, sub-section (d) "Openness of the OSP to negotiating mutually acceptable contractual and SLA provisions"

We request CBI to provide more details on the expectations here.

- Page 29, Section 6.2, sub-section (d): "Periodically19 review the "financial health" of key OSPs, providing critical or important services, over the lifecycle of the contract. Even the largest of the OSPs can fail; and…"

We note that the requirement is trigged by criticality and not IRR. We would request Clarity on whether due diligence is expected to be complete both before and at end of contract stages.

7. Contractual Arrangements and Service Level Agreements (SLAs)

The Central Bank expects that, arrangements with OSPs are governed by formal contracts or written agreements, preferably that are legally binding. These should be supported by Service Level Agreements (SLAs).

Clarification is required as to whether this is applicable to C/I arrangements only. We note that the opening paragraph of Section 7 and Section 10.2 (q) would suggest that this applies to all agreements. We would recommend that this is restricted to C/I as per the approach in the EBA Outsourcing Guidelines at paragraph 75.

7.1 *General Requirements No Comments*

7.2 *Termination Rights No Comments*

7.3 *Access, Information and Audit Rights*

The Guidance states that regulated firms are expected to exercise their access and audit rights, determine the audit frequency and areas to be audited using a risk-based approach and in doing so adhere to relevant, commonly accepted, national and international audit standards. Can we assume that records in relation to audit maintained in the outsourcing register will be sufficient to evidence this point?

7.4 *Review of Agreements No Comments*

7.5 *Non-Critical or Important Outsourcing Arrangements No Comments*

8. Ongoing Monitoring and Challenge

8.1 *Monitoring of outsourcing arrangements: No Comments*

8.2 *Internal Audit & Independent Third-Party Review*

The Guidance states at Section 8.2, second sentence (page 35) that "Regulated firms must also ensure that assessment of the effective performance of the arrangement and of the controls to mitigate associated risks, forms part of its third line of defence assurance programs, via its internal audit plan". BPFI members assume the testing of operation by the OSP could be completed by an independent party but not explicitly be part of the internal audit plan.

8.3 *Use of Third-Party Certifications and Pooled Audits: No Comments*

9. Disaster Recovery and Business Continuity Management

CBI sets out a comprehensive list of steps that firms should undertake when designing and implementing disaster recovery and business continuity measures as they pertain to or include outsourced arrangements. While we recognise the applicability of many of these requirements, we believe that they should be limited to outsourcing involving critical or important functions. For outsourcing, which is not critical, the resilience of the OSP should be determined within the financial institutions' risk appetite frameworks.

We note that several of the requirements laid out in Section 9 should not apply to all outsourcing arrangements and some of them exceed the EBA requirements:

- Safe Harbour backups: The requirement to create isolated "safe harbour" backups should not be applicable to all cloud arrangements. We refer to our comments regarding section 5.3 page 23. Offline or isolated data backups serve a narrow purpose and are often not applicable in a recovery situation. We are familiar with the US Sheltered Harbour programme but note that this is strictly limited to customer account data covered by deposit protection insurance. The utility of such a programme outside of this specific case is highly questionable. We suggest instead that this requirement be altered to focus on the outcome that the CBI wants financial institutions to achieve, namely that they have the ability to recover data in the event of a compromise to confidentiality, integrity and availability of their critical data and systems. We believe a focus on the outcome will allow firms the necessary freedom to determine how best to achieve the desired result for their particular systems and in line with the rapid evolution of technology.

- Co-ordinated testing: The requirement to conduct coordinated testing is disproportionate and would be difficult to achieve for OSPs serving multiple clients. We note that only the largest of OSPs would be in a position to provide this service and we are concerned that this would have the de-facto result of excluding smaller OSPs from servicing the financial sector. This would mean a reduction in financial institutions access to innovative technology and could also contribute to further concentration in a small number of providers. We suggest instead that financial institutions be allowed to rely on the business continuity testing performed by the OSP provided that the OSP is able to adequately evidence this testing and demonstrate that it has been conducted at a level the financial institution deems appropriate to its risk appetite and impact tolerance requirements.

We note that Section 9 (b) (page 38) refers the reader to Section 10.1 for exit strategies. We believe the reference should instead be to Section 9.1.

9.1 *Exit Strategies*

We note that some authorities have recognised the limitation of exit plans in the case of intragroup arrangements. In their recent paper on Outsourcing and Third-party Risk, the FSB noted that "Developing and executing exit strategies can be challenging in practice in the case of certain intra-group arrangements. Some jurisdictions (e.g., Germany) allow the establishment of specific processes to "be waived in the case of outsourcings within a group or within a network of affiliated FIs" on proportionality grounds.[1] We believe this approach is appropriate. Furthermore, we note the recent approach of the PRA, which acknowledges that for intragroup arrangements, firms' exit options might be considerably more limited than in other scenarios but that entities should take reasonable steps to try to identify options.[2]

Please also refer to our comments under Section 4.2 in relation to exit plans.

10. Provision of Outsourcing Information to the Central Bank of Ireland

10.1 *Notifications & Reporting*

The Guidance states that notification requirements are 'in line' with the EBA guidance and set out that 'it should not be inferred from the expectations relating to Notifications that the Central Bank is creating a pre-approval process, where such a pre-approval is not an existing legal requirement. The Guidance does not supersede existing sectoral legislation, regulations and guidance on outsourcing, but rather supports and complements them by setting out aspects of good practice for the effective management of outsourcing risk in all its forms.'

BPFI members support a notification approach and agree with the CBI that it should not look to create a pre-approval process. However, we note that there are some statements in the Guidance that run counter to the suggestion that the process is not pre-approval. For example, the consultation document points out that sufficient time should be given 'to permit appropriate supervisory consideration of the risks associated with the proposal'. Furthermore, the list of requests that the CBI notes that it may require firms to undertake as part of early-stage dialogue could be construed as effective 'pre-approval'.

[1] FSB, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, Nov. 2020, p.28.
[2] PRA, at 11.5 - https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021/march/ps721.pdf?la=en&hash=6C70BEE48B89D7965D43894DB848FC41CD5EC6C0

We would recommend that the CBI seeks to avoid the introduction of requirements that will create an effective pre-approval process. Provided that firms have appropriate control and governance requirements in place in line with existing regulations, additional roadblocks should not be put in place. This will be of particular importance for any outsourced functions that are time critical and could therefore have implications from a firm and market resilience perspective if they are held up as part of approval processes.

We would also recommend the following:

- Request supervisory teams publish notification templates for submission of notification of proposed or changing arrangements; and
- Notification templates are consistent with the notification requirements as set out in EBA. Any additional information required by the supervisory teams should be set out in separate sections to what is under EBA paragraph 54; and
- The introduction of a set time limit in which the CBI can respond with requests for additional information.

In relation to termination of critical or important outsourcing arrangements, we believe that clarification would be helpful as to the circumstances which would warrant notification to the CBI, as this is limited in the current EBA guidance. Also, would change of a critical arrangement to a non-critical arrangement trigger a notification requirement to the CBI?

10.2 *Maintenance and Submission of Registers*

The CBI expects that each Regulated firm will establish and maintain an outsourcing register (broadly in line with EBA). The submission of the data contained in the Registers (Databases) of firms will be by way of a periodic Regulatory Return. The frequency and timing of such returns will be specified to sectors by way of an Industry Letter.

Firstly, as a general observation we believe that consistency with the EBA O/S register should be maintained as much as possible in order to prevent the need for local deviations within the EU. Firms should be able to rely on an EBA register that is consistent across all EU entities. Register requirements set by the CBI deviate from EBA register requirements in their guidelines, in terms of scope (future arrangements), difference in format/definition of data points (i.e. Location of Data to include City/Town, Regulator of OSP to be reported), as well as other reporting requirements over and above EBA GL. We would therefore recommend that:

- The CBI accept the EBA register in the first instance. Any requests for additional information should be separate and distinct as set out under EBA 54 and 55.

We would also recommend the following:

- Future Arrangements: The return should be a register only of current outsourcing arrangements at time of submission. We request removal of "future outsourcing arrangements" from the first sentence of page 45.
- Terminated Arrangements: It is not clear that a 'record of terminated arrangements would provide additional value to the CBI given that there are already requirements to notify the CBI of termination of critical or important outsourcing under Section 10.1.1 (f). While we acknowledge that firms should retain records in relation to terminated arrangements, we believe that this should not be included with a periodic return.
- Arrangements to 'other regulated entities': Page 58 requires firms to answer, "Does the firm provide outsourcing services to other regulated firms?" Clarity is required as to what "regulated firms" are in scope here. If this is only in relation to entities in Ireland, the CBI has this information already from the regulated firm's requirement to complete the regulatory return (which would include details of any firms regulated in Ireland as service providers). We would emphasise that this proposed obligation is an outlier as it imposes an obligation to firms in their capacity as a service provider of outsourcing services as opposed to a recipient.
- SLAs: BPFI requests that the requirement to provide detail on "Are Contracts / Written Agreements supported by SLAs" be limited to critical or important outsourcing activities.

Contacting Us:

If you would like to further discuss details of this submission you can contact us at:

Dr Ali Ugur, Chief Economist and Head of Prudential Regulation
Banking and Payments Federation Ireland
Email: ali.ugur@bpfi.ie
Tel: 014748814