Banking & Payments Federation Ireland

BPFI Response to the Central Bank of Ireland Discussion Paper on Outsourcing

January 2019

www.bpfi.ie

Introduction

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 comment on this discussion paper and look forward to the proposed conference to be organised by the Central Bank of Ireland in the first quarter of 2019, noting that the recent EBA draft consultation is likely to be finalised during the same period. In this context, we note that the paper references the potential for further guidance or policy to be issued by CBI. However, it is not clear to us as to whether this will incorporate additional requirements to those already included in the new draft EBA Outsourcing Guidelines.

Outsourcing arrangements are widely utilised by the banking industry as they contribute to the efficiency and to the competitiveness of banks' business models in addition to enabling them to focus on their core business with access to skills and services that may not be available in house.

In section 1 we outline some of the issues that the BPFI response to the recent consultation on draft EBA guidelines covered, as we believe they are still relevant in the context of this discussion paper. Section 2 covers some questions in relation to the minimum supervisory expectation outlined in the first part of the discussion paper under various headings. Section 3 concludes with comments on the questions raised in the paper in relation to current and future risks as well as questions in order to facilitate further discussion on issues raised.

Section 1- General Comments

Definition of outsourcing is too broad and there is a need for additional examples and guidance of what activities are not considered outsourcing, where there is a risk of many activities performed by third parties on behalf of regulated institutions as outsourcing within the current EBA guidance. We believe that services or activities within the scope of outsourcing should reflect two main features; that they are performed on an *ongoing basis* in the course of an *institution's ordinary business*. The acquisition of goods, services or utilities that are not normally performed by financial institutions on an ongoing basis during the course of their ordinary business should not be considered outsourcing, perhaps the scope should be limited to "critical and important operational functions" as in the MiFID II legislation.

Intra-group outsourcing arrangements are widely used by the banking industry where they provide an essential platform for the efficient allocation of tasks and skills across banking groups' entities, thus contributing to their competitiveness. BPFI members believe that intragroup outsourcing and the level of centralisation of functions at group level should be recognised reflecting the difference in risk profile between intragroup outsourcing and outsourcing to third parties and hence intra-group outsourcing should not be subject to the same level of compliance and reporting obligations as third-party outsourcing agreements. The degree of integration reached within many banking groups, where centralized functions at group level act as a service provider for the other entities of the group makes the proposed stricter requirements on documentation, due diligence, concentration risk and exit strategy prove to be less relevant or even irrelevant from an intra-group perspective. For example, intra-group outsourcing should be recognised in the context of recovery and resolution plans and shared servicing agreements rather than applying replacement tests for third-party outsourcers. In the context of an intra-group outsourcing, material deterioration in service is more likely to be resolved by escalation and management intervention, rather than moving to a different service provider.

We believe that **exit strategies** in the context of outsourcing are less relevant for for certain business models. The existence of robust group recovery and resolution frameworks should be considered when evaluating exit strategies where many financial institutions would have opted for a "single point of entry" resolution strategy at the group level, where the parent company ensures the continuity of the critical functions performed by its subsidiaries. Under this pattern, subsidiaries outsourcing critical

or important functions to their parent company rely on the business continuity plan and on the exit strategies of their parent company.

Section 2- Minimum Supervisory Expectations

Governance Findings:

The paper outlines that the CBI expects that regulated firms give due consideration to their outsourcing strategy and are in a position to evidence this. The paper states that the existence of a Board approved outsourcing policy is not of itself indicative of whether the impact of outsourcing on the firms' ability to deliver its core services is appropriately understood at board level.

1. BPFI members assume that a board approved and documented Outsourcing Strategy is sufficient. Please provide guidance as to how to approach this in a demonstrable fashion.
2. Can the CBI provide further clarity on the definition of "partnerships" and given that it is specifically included in the paper?
3. "Boards have appropriate oversight and awareness of current & proposed outsourcing arrangements"……. At what point during the creation of a new outsourcing arrangement should a board, or their delegated authority, be engaged for awareness and oversight? Is it the CBI's expectation that boards should agree upfront that particular services require outsourcing in the first instance and thereafter commence the creation of a new intragroup contractual arrangement in support rather than ratify submissions made by an underlying entity/Business Line via a governing committee, having considered all relevant factors, seeking such to be affected?
4. Where does the concept of materiality come into focus in relation to the board oversight and awareness? Please provide further guidance as to how to approach this matter in terms of board oversight and awareness, and timing of same.

Risk Management Findings:

1. From a cyber security perspective, what are CBI's expectations in respect of embedding this in respect of OSP oversight aside from the inclusion of standard contractual language and confirmation of OSP provider's adherence with the regulated firm's policy requirements given the evolving/maturing cybersecurity risk profile?
2. Please provide greater clarity on the "criticality and importance of service" methodology and which "relevant sectoral regulations and guidance" is referred to in this statement.

Business Continuity Findings

1. What are the other issues that BPFI members need to be mindful of where the expectation is laid out " particularly in the context of new and evolving technologies, trends and risks" - What are the CBI views in this regard?
2. "Regulated firms have back up measures in place and consider, plan and test scenarios for exit strategies from outsourcing arrangements." Please clarify what the CBI expectations are on how the service user would demonstrate that they've considered, planned and tested these defined exit strategies or a selected scenario documented within? What detail should be applied and how frequently this should be carried out, e.g. 3-year cycle / risk-based approach / annual / half-yearly / quarterly?
3. "Skills and expertise are developed and maintained so that functions can be taken back in-house.....". What are the CBI expectations in this regard and what demonstrable evidence is required to support evidence of same?

Section 3- Key Risks and Evolving Trends

Sensitive Data Risk

- How are regulated firms ensuring that they have sufficient knowledge/ expertise within their own organisation to effectively challenge and gain assurance that their data is being managed securely by OSPs, including CSPs (how and where it is being stored, processed, used, located etc.)?

Most BPFI member banks would have dedicated functions to assess Third Party security controls during all stages of third-party management (RFP, Contracting, On boarding, Ongoing, Exit). The team members of the functions are generally information security professionals with the relevant experience and qualifications. The processes would follow industry standards and best practices e.g. use of ISO, NIST Controls and Cloud Security Alliance.

Third parties would generally be assessed against a series of cloud security questions, for which controls align to internally defined policy. For third parties where a control is not being met in the area of cloud security, findings are created and tracked until remediation. The cloud security questions cover areas of access management, application security, encryption standards, data integrity, incident monitoring and response, network security, and systems security. In addition, certain evidence artefacts are reviewed to gain assurance that cloud security controls are consistent with internally defined policy.

For BPFI members as part of a group, relevant parent/group policies are completely aligned with the local regulated firm policies (e.g. Data Protection). In this regard legal teams would be engaged and advises in relation to data processor agreements and standard contractual clauses that are required to be put in place. Contracts entered into with designated OSPs are required to be in full compliance with relevant regulatory expectations including CEBS Guidelines / EBA Guidelines / GDPR Requirements to ensure required clauses are in place e.g. data protection, event management, etc. If a deviation is noted (e.g. Global OSP refuses to amend contract) then a contract variance is created, approved via the governing process and action documented to mitigate same.

In addition, for some member banks, data location is clearly marked for consideration in their cloud policy documents, where they exist. All third parties must disclose locations of where regulated firm data is stored, where this data can be assigned classifications and risk levels. Third parties then can conduct external audits that include physical controls as well as backup and recovery controls and where required evidence of external cloud audits are reviewed by a functional team.

BPFI members would like to get further guidance as to whether the CBI intends to align their expectations to global / EBA standards e.g. acceptance of independent certification of certain types of OSPs. For example, does the CBI expect SOC type reporting from 3rd parties as part of the ongoing monitoring and oversight of their adherence to the required security standards?

- What issues/ challenges are regulated firms encountering in gaining assurance that their sensitive business and customer data is being managed securely in outsourcing scenarios?

1. The same assessments are being asked by each supervised firm of the Third Parties. The Third Parties are challenged with producing similar information in different formats. This is inefficient for all stakeholders.
2. The independent audits and accreditations that the Third Party maintain such as ISO 27001 and SOC 2 Type II reports are not seen as sufficient assurance by supervisory authorities.
3. There may be a number of functions within one regulated entity with information and assessment requests that must be scheduled with the Third Party.
4. There is little practical guidance by supervisory authorities on structuring the assessments of Third Parties in a way that can be clearly used by regulated entities.

Concentration Risk

- How are regulated firms seeking to reduce their exposure to concentration risk both from the perspective of providers and geographical locations?

Concentration risk analysis and awareness is required per regulated firm policy, as part of due diligence activities. However, guidance is leading towards the fact that large suppliers of IT / OSPs are or could become a single point of industry failure when many institutions rely on the same provider. In addition, some OSPs may hold significant leverage owing to the nature of services provided (i.e. lack of substitutability).

BPFI members recognise the risks arising from concentration of services form a single third party, sector or country, and the impact to individual banks as a result of a failure of that third party, sector, or country. Members are aware of this risk and consider concentration risk when selecting suppliers, ensuring that, where appropriate, there is sufficient diversity in its supply chain to protect their bank as a result of a failure. In this regard, considerations include, but are not limited to, substitutability of

service; number of other providers in the market; ease of transfer of service; banks' reliance on suppliers; suppliers' reliance on banks and number of services provided to banks or supported by the third party.

While some plans may be in place (e.g. shorter OSP contract duration, contract variance in place, substitutes identified, stringent ongoing monitoring, third parties on critical watch report) to mitigate the risk of consolidation of service providers in the market place, it would be beneficial to obtain further guidance in respect of CBI's expectations in respect of mitigating OSP concentration risk over and above those already noted. In this context, it would be useful to get further detail about the current CBI view on concentration risk for the Irish economy and whether the CBI will be providing further guidance and support on this issue given the fact that for some key service areas there are very limited or no viable alternatives in Ireland. For example, does the CBI envisage introducing a cap or level, for the broader industry, for a particular sector or within an OSP group (e.g. intragroup, Cloud Service Providers) in order to mitigate any sovereign or sector risk that may only be fully visible to the regulator?

At a macro level though BPFI members believe that financial regulators and supervisors will need to rely on more than the contractual relationship between providers and regulated firms, for example through monitoring of the third-party providers however it is clear that further debate is necessary in this area. It would be beneficial to obtain further guidance in respect of CBI's expectations in respect of mitigating other forms of concentration.

- How are regulated firms addressing concentration risk whereby they are outsourcing to OSPs who provide services for a large proportion of their sector? Of particular interest is how regulated firms are dealing with concentration risk where there are limited numbers of providers of niche services such as CSPs?

Ireland is a small economy and compared to other jurisdictions, there is limited choice in certain sectors for delivery of some banking services that would be considered material, for example, Cash in Transit. There are a limited number of providers with the capability of providing such services to the Irish banking industry, and this creates a risk not only to banks, but is a sectoral risk to all banks in Ireland as for example these companies also serve the retail sector as well as are involved in transit of some of the state payments. However, in order to manage and mitigate this type of risk, for example in the case of cash services, an industry plan (between a number of Irish banks and financial service providers) had been developed in conjunction with the Central Bank.

Concentration risk to CSPs is relevant in financial services, but it is likely that it will grow in importance for other important sectors as usage increases and perhaps there is a role for regulators across different sectors to work together in relation to overall risk mitigation measures in the event of for example system failure or a catastrophic event.

- Do regulated firms have views, as to how systemic concentration risk related to outsourcing, can be effectively monitored and managed by both regulated firms in all sectors and the Central Bank?

BPFI members believe that there may be benefit in sharing of information of outsourced services, or industry plans relevant to regulated services, provided by third parties to banks, that could be used by banks and the CBI to better understand the concentration risk posed by third parties, sectors, or countries. For example, for critical services industry plans can be developed in conjunction with the BPFI/CBI. We see examples of this abroad, e.g. US based regulators oversee and assess financial technology providers that have systemic importance.

Offshoring and Chain Outsourcing

- Given the significant volume of offshoring to the UK what preparations are regulated firms undertaking to prepare for Brexit and what related challenges are envisaged in terms of their outsourcing arrangements?

Significant number of BPFI members would have Brexit projects and examined their supply chain, and identified suppliers providing services from the UK to their organisations, or from other jurisdictions to operations in the UK. These projects would have a specified program of work elements of which involve but are not limited to risk assessment and scenario planning, and from a chain outsourcing perspective includes obtaining information from selected OSPs regarding their readiness in respect of Brexit i.e. Hard Brexit or no deal scenarios.

Data transfer between the UK and the EU is seen as a significant risk, and members are working on measures to put protection in place in the form of additional model clauses to existing contracts. While the cost of doing business with UK is likely to increase as a result of Brexit, BPFI members do not envisage significant disruption from a resourcing (or movement of staff) perspective.

What steps are regulated firms taking to ensure they have full sight of any chain outsourcing which may be occurring within their outsourcing arrangements and how are they managing risks associated with this?

BPFI members currently rely on the 2006 CEBS requirements when considering material OSPs and chain outsourcing risk, and utilise standard contractual language or the instigation of contract variances if necessary.

Institutions are only engaged with the main contractor and they would be unlikely to be able to obtain the relevant information or negotiate the type of contractual clauses for chain outsourcing. Using regulatory requirements in order to understand outsourcer's supply chain may not work in practice.

An alternative approach may be to, for example, allow financial institutions conduct an assessment of the main provider's third-party approval process with reference to accepted standards (such as relevant ISO standards) which can also provide consistency across the industry with respect to way the potential risks associated with chain outsourcing are mitigated.

BPFI members would like clarity as to whether the CBI intends to provide any further guidance on the best way to apply the risk management principles into the OSP supply chain and sub-contracted services, where the buyer of the services may not have the contractual rights to gain access for assurance activity, in particular with CSP? In addition, it will be useful to get further guidance on the length of the chain to be understood and clarity of the differences between supply chain/sub-contracting.

- How are firms ensuring that contractual rights of access are the same with all parties to a chain-outsourcing arrangement, as those granted by the primary third party OSP?

This would be part of institutions' outsourcing programme which is done through contract negotiations and annual reassessments.

Substitutability

- What issues/ challenges are regulated firms encountering when assessing substitutability and exit strategies? How are these being addressed?
- What are the risks / challenges where there is no substitutability or it is not possible to bring the service back in house? How are these being addressed?

We are not sure as to what extent a regulated firm is expected to have pre-implemented their defined exit strategy, particularly in the context of recovery and resolution planning as outlined in the first section of this response. It is important to emphasize that depending on the regulatory expectations, this may have significant resourcing/operational impact to establish and test for all outsourced relationships.

It would be useful to get additional guidance regarding partial or full substitutability (e.g. if service is not regulated/not material or mission critical. For example, can a regulated entity apply a risk-based approach methodology using materiality, mission critical process, etc once which is documented and approved by the Board/delegated governing authority with a view to applying this approach for intragroup OSPs?

Some of the areas of concern around substitutability include;

- Testing of BCM.
- Periodic supplier Criticality reviews –
- Periodic review/assurance of Controls in place –
- Industry view of supplier risk (eg: solvency)
- Termination agreements and exit plans are developed.
- BCM testing.
- Initial risk assessment to make decision.

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

[redacted]