SHCOG Securities Houses Compliance Officers Group

Outsourcing Risk

30 June 2021

Agenda

- Current EU and UK Regulatory Expectations
- Elevated Focus on Interaffiliate / Intragroup Outsourcing
- Governance expectations including the role of the SMFs and demonstrating oversight of services provided by the Group / Head Office
- Key Risks Associated with Outsourcing and thoughts on how to manage them
- What are ‘reasonable steps’ when it comes to demonstrating appropriate governance and management of outsourced arrangements

Current EU Regulatory Expectations

EBA Guidelines on outsourcing arrangements (25 February 2019)

- The guidelines apply from 30 September 2019 to all outsourcing arrangements entered into, reviewed or amended on or after this date. For existing outsourcing arrangements institutions should review these with a view to ensuring that these are compliant with these guidelines. Where the review of outsourcing arrangements of critical or important functions is not finalised by 31 December 2021, institutions should inform their competent authority of that fact, including the measures planned to complete the review or the possible exit strategy.

- Definition: 'Outsourcing: means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself'

- The guidelines include requirements that aim to ensure:
  a. effective day-to-day management and oversight by the management body;
  b. a sound outsourcing policy and processes that reflect the institution's strategy and risk profile;
  c. effective and efficient internal control framework;
  d. proper identification of critical or important functions and suitability of potential service providers;
  e. that all the risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, reported and, as appropriate, mitigated;
  f. protection of customer data across the whole institution, including the outsourced functions;
  g. appropriate plans for the exit from outsourcing arrangements of critical or important functions, e.g. by migrating to another service provider or by reintegrating the critical or important outsourced functions; and
  h. competent authorities remain able to effectively supervise institutions.

Current UK Regulatory Expectations

Outsourcing remains a key area of focus for UK regulators in particular in light of it's importance in the context of operational resilience and the stability of UK firms and UK markets. There have been number of recent publications in this area with the approach largely aligned with EBA guidelines

- Following the finalisation of the EBA's guidelines on outsourcing in February 2019, the FCA notified the EBA that they would comply with the EBA guidelines on outsourcing. In line with this the FCA has stated that they expect firms to continue to comply with the guidelines, to the extent they remain relevant, now that the UK has left the EU.

- The FCA recently updated their website to modify the notification requirement noting that "firms are not expected to report to us on their progress towards meeting the timeline of 31 December 2021 in the EBA guidelines on legacy outsourcing arrangements".

- In scope UK firms should instead aim to review any outstanding critical or important outsourcing arrangement at the first appropriate contract renewal following the first renewal date of each existing outsourcing arrangement or revision point. Where arrangements of critical or important outsourcing arrangements have not been finalised by 31 March 2022, firms should inform us.

- This revised timeframe aligns with that of the FCA's final operational resilience policy (PS21/3). The approach to these guidelines aligns with that of the PRA as set out in PS7/21.

Elevated Focus on Interaffiliate / Intragroup Outsourcing

Examples from the Central Bank of Ireland

"….regulated firms may be able to exercise more control or influence in respect of the management of intragroup outsourcing arrangements; although the opposite may also be the case"

"….while the risks associated with both intragroup and third party outsourcing are predominantly the same, intragroup outsourcing also presents unique risks"

"….Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group and it is important for regulated firms to note that intragroup outsourcing and third party outsourcing are subject to the same supervisory expectations"

Examples from the FCA

"….Firms with intra-group arrangements are required by outsourcing legislation, and the FCA rule, to meet the same requirements as outsourcing to an external third party"

"….Firms should not treat it as being less risky… [but] may consider the extent to which they influence and control their third-parties where those parties are members of the same group so that risks can be identified and managed effectively.

"…. A firm's arrangements with third parties falling outside the definition of 'outsourcing' may not be subject to specific requirements on outsourcing. They are however within the scope of the FCA's rules and guidance, particularly on governance, risk management and systems and controls"

Key Areas of Regulatory Focus:

- Awareness of the Scale of Outsourcing (Volume, Value, Criticality, etc.)
- Concentration Risk (Often significant and international Concentration Risk, which needs to be understood and mitigated)
- Interaffiliate Sub-Contracting to Third Parties (Understanding the ultimate external Third Party exposure)

Key Risks Associated with Outsourcing and thoughts on how to manage them

Key Risk Associated with Outsourcing:

1. Concentration Risk - Risk of loss arising from multiple outsourcings to the same service provider and/or by outsourcing critical or important functions to a limited number of service providers

2. Sub-Contracting Risk - Risk that the regulated firm does not ensure that the Outsourced Service Provider oversees and manages the activities of the subcontracted Outsourced Service Provider to ensure the fulfilment of all services in line with the original outsourcing contract and relevant service level agreement

3. Offshoring Risk - Risk associated with outsourcing to another legal jurisdiction (regulatory environment, political environment, etc)

4. Substitutability Risk - Risk that the Outsourced Service Provider is unable to continue to provide the contracted service, resulting in a requirement to transfer the outsourcing arrangement in house or to another service provider

5. Sensitive Data Risk - Where data is being transmitted to the Outsourced Service Provider, there is a risk of data loss, alteration, corruption or of unauthorised access while in transit.

Growing Focus on Climate and Environment Risk:

Risk of offshore location being subject to extreme weather or other environmental events and potential impacts on ability to continue providing service

Managing the Key Risk Associated with Outsourcing:

Service Level:

- Initial Risk Assessment (i.e. pre-outsourcing)
    1. Data Collection (rationale for responses), including risks associated with Outsourcing the Service
    2. Scenario Analysis
    3. Conclude with an overall Risk Assessment outcome
    4. Document additional mitigants and/or controls as required
    5. Second line Review and Challenge

- On-going Risk Assessment (i.e. post outsourcing)
    1. Review and Update Initial Risk Assessment

Firm or Legal Entity Level:

- Assessment of Inherent Risk, Control Effectiveness and Residual Risk for Key Risks
    1. Concentration Risk
    2. Sub-Contracting Risk
    3. Offshoring Risk
    4. Substitutability Risk
    5. Sensitive Data Risk
- Scenario Analysis, Aggregate Service Level
- Key Performance Indicators
- Risk Appetite
- Regular Reporting to the Senior Management Team and Board (Volume, Value, Criticality, etc.)

Governance expectations including the role of the SMFs and demonstrating oversight of services provided by the Group / Head Office

As noted elsewhere, outsourcing requirements are not limited where the arrangement is intragroup. Specific outsourcing obligations may not directly apply to intra-entity arrangements but many of the governance expectation will still apply. Areas to consider include:

- SMFs should consider whether outsourcing impacts on their ability to perform their prescribed responsibilities and if so ensure they can demonstrate appropriate oversight of those requirements and that they and their teams are appropriately trained to exercise that oversight
- For PRA regulated firms the 'responsibility for the firm's performance of its obligations under Outsourcing' is a prescribed responsibility and will need to be assigned to a senior manager. In considering the allocation of this role, firms will need to consider which senior manager is best placed to hold the role given the range of outsourced activities. Firms should also consider what oversight framework is required to support the designate senior manager.
- SYSC 3.2.4: A firm cannot contract out of its regulatory obligations an needs to develop a control framework that aligns to the nature, scale and risk of operations
- SYSC 8.1.1: Firms should take reasonable steps to avoid undue additional operational risk when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities
- SYSC 8.1.3: Where a firm relies on a third party for the performance of operational functions which are not critical or important for the performance of relevant services and activities on a continuous and satisfactory basis, it should take into account, in a manner that is proportionate given the nature, scale and complexity of the outsourcing
- The list goes on.. Long story short, it is critical for firms to be able to demonstrate appropriate demonstrate a clear framework for the oversight of services provided by both true third parties and other parts of their group

What are ‘reasonable steps’ when it comes to demonstrating appropriate governance and management of outsourced arrangements

- Documented Outsourcing Policy and Strategy
- Clearly Defined Roles and Responsibilities (Service Receivers, Service Providers, Second and Third Line of Defence)
- Comprehensive Initial / Pre-outsourcing Risk Assessment and On-going Risk Assessment process
- Detailed Description of Outsourced Arrangements
- Well documented Criticality / Materiality Assessment, aligned to Regulatory Expectations
- Documented Scale of Outsourcing (Volume, Value, Criticality, etc.)
- Regular update to Management team on the Key Risks associated with Outsourcing
- Consideration of Climate Risk Impacts
- Scenario Analysis that assumes failure of the Service Provider
- Key Performance Indicators plus other more Qualitative Indicators
- Documented Exit Strategy
- Service Delivery Council / Committee
- Outsourcing Risks documented with the Risk Identification process
- Consider Risk Appetite Metrics, particularly if Outsourcing is considered a Material Risk

What can happen when it goes wrong? (1 of 2)

Both the FCA and the PRA have taken enforcement action against firms for outsourcing-related failings. Enforcement to date has been at the NCA rather than European level.

R Raphael & Sons plc (2019)

The FCA and PRA each issued separate fines to R. Raphael & Sons plc ("**Raphaels**"), for failing to manage its outsourcing arrangements properly between April 2014 and December 2016. This was the second fine of this kind issued to Raphaels by the PRA. The Final Notices were each issued on 29 May 2019, and the fines were for £775,100 and £1,121,512, respectively.

The joint FCA and PRA investigation identified weaknesses throughout the firm's outsourcing systems and controls, which Raphaels ought to have known about since April 2014. These included a lack of adequate consideration of outsourcing within its board and departmental risk appetites, the absence of processes for identifying critical outsourced services, and flaws in its initial and on-going due diligence of outsourced service

This case underlines the importance of establishing proper outsourcing systems and controls, including putting in place contractual documentation that does more than just recite general regulatory requirements, engaging in appropriate initial and ongoing due diligence of service providers, and ensuring appropriate risk identification and management processes. The case also stresses the importance of understanding the business continuity arrangements of service providers, what to expect during a disruptive event, and how communications concerning such events will be managed.

What can happen when it goes wrong? (2 of 2)

Liberty Mutual (2018)

The FCA published a Final Notice to Liberty Mutual Insurance Europe SE ("**LMIE**") on 29 October 2018, fining LMIE £5,280,800. LMIE had outsourced the performance of administrative functions associated with mobile phone insurance to a third party, including its claims and complaints handling functions. The FCA found that LMIE breached FCA Principle 3 (Management and Control) and Principle 6 (Customers' Interests) as the company had failed to ensure that it had adequate systems and controls in place to oversee the third party contractor, resulting in poor results for customers.

Specifically, LMIE did not undertake an adequate risk assessment in relation to the outsourcing, nor did it adequately plan for ongoing monitoring of the arrangements. Although the arrangements were overseen by the Compliance Function and the Audit Committee, there was a lack of oversight from the board and senior management, resulting in thousands of customers unfairly being denied cover for their claims.

This case demonstrates the importance of having proper oversight of outsourced service providers' activities, understanding their business model, and addressing concerns at an early stage. The case also emphasises that it is not acceptable for a firm to leave a third party to design such an offering, without the firm having adequate systems and controls in place to ensure that the third party's activities comply with the relevant regulatory expectations.