Position Paper

Response to FSB consultation on outsourcing and third-party relationships

Our reference:	COB-TECH-21-003		
Referring to:	FSB discussion paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships		
Contact person:	Arthur Hilliard, Senior policy advisor, Conduct of Business	E-mail:	Hilliard@insuranceeurope.eu
Pages:	4	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the Financial Stability Board's discussion paper and the opportunity to provide stakeholder feedback on regulatory and supervisory issues relating to outsourcing and third-party relationships. A well-balanced approach must be found which provides additional clarity to users of third-party services, without putting unduly burdensome regulatory requirements on users or providers of such services. The intention of any work in this area should therefore be to help provide the necessary clarity for financial institutions to enable them to adopt and reap the benefits of third-party services, such as cloud computing, while also ensuring that any risks are appropriately identified and managed.

Questions

Q.1 *What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?*

Q.2 *What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?*

Q.3 *What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?*

Q.4 *What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?*

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

Key challenges

As regards the key challenges faced by financial institutions, as referred to in Q.1, they are often based on issues related to non-transparent contractual agreements (eg with regard to sub-outsourcing), concentration risk due to lack of providers, or a significant imbalance of negotiating power making it difficult to ensure appropriate sectoral regulatory constraints are reflected in their contractual agreements. In many cases, third-party providers offer their standard terms on a 'take-it-or-leave-it' basis, leaving very little, if any, opportunity for financial institutions to negotiate terms.

In the context of outsourcing to cloud service providers, an additional challenge that is regularly encountered by the insurance industry relates to the fact that the cloud service provider will generally refer to its own standard terms and conditions regarding the right to unilaterally change the terms of service. This is often with very little or insufficient notice for the insurer to assess the changes and, if necessary, initiate an exit from the contract. While not an issue that is directly covered by the existing regulatory framework on outsourcing, Insurance Europe would welcome further consideration of this problem to ensure that financial institutions are provided with sufficient time to assess any proposed changes to the terms and conditions of service and, where deemed necessary, to allow for an orderly withdrawal from the outsourcing arrangement.

Insurance Europe has highlighted below the main contractual areas where insurers regularly face challenges in their dealings with third-party service providers, as well as possible ways of addressing these challenges, as addressed in Q.2 and Q.3).

Challenges and possible solutions

Sub-outsourcing

The sub-outsourcing of any elements of a service to other providers should be properly notified to the financial institution in due time to allow it to make its own assessment of the adequacy of the sub-outsourcing. All relevant information about the third party should be provided to the financial institution.

Where a service provider sub-contracts elements of the service to other providers, this should not affect the services provided under the agreement, and appropriate arrangements should be in place for the orderly transfer of the activity, data or services from the sub-contractor to another service provider if necessary.

The service provider should retain full accountability and oversight for the services sub-outsourced. The agreement should also indicate the conditions to be complied with, eg that the sub-contractor will also fully comply with the relevant obligations of the service provider, such as any audit/access rights and security of the data.

While it may be difficult for financial institutions to stipulate a right of approval in their agreements with third parties, at the very least it should be possible for financial institutions to have the contractual right to terminate the agreement without penalty in the case of sub-outsourcing that might impact its risk assessment of the service provision.

Security of data

The quality of the service delivered by a third-party service provider (eg cloud service provider) is dependent on its ability to appropriately protect the confidentiality, integrity and availability of the data and of the systems and processes used to process, transfer or store this data. For example, cloud service providers

would need to be able to ensure that they meet the data-related demands of any relevant requirements, such as the General Data Protection Regulation (GDPR), and to reassure financial institutions that the cloud solution they offer is performed in a sufficiently safe and secure environment. Third-party providers therefore need to ensure they comply with minimum security standards that are in line with relevant European and national regulations.

Access and audit rights

Providing for regular on-site inspections of service providers is not necessary to achieve supervisory or monitoring objectives. On-site audits give limited insights into service performance — it would be more relevant therefore to focus on the provider's compliance with applicable laws and information security standards. For example, rather than focusing on physical on-site inspections, which become less relevant given the remote nature of services such as cloud computing, it should be possible for supervisory authorities or internal audit functions to rely on independent assurance by third-party certification bodies or compliance with relevant standards (see below point on certification), in order to use audit resources more efficiently.

Contingency plans and exit strategies

Contingency plans and exit strategies form an important part of any outsourcing arrangement. It should be possible for financial institutions to be able to exit outsourcing arrangements, should they wish to, without undue disruption to their provision of services or their compliance with the regulatory regime.

To avoid potential vendor lock-in situations, it is important therefore that third-party service providers facilitate the prompt transfer of data to alternative service providers or back in-house following contract termination to ensure business continuity during the transition phase. This could involve an appropriate minimum transition period with an obligation to ensure service continuity following termination in order to avoid the risk of disruption. It should be ensured that once the data has been transferred back to the financial institution, it will be completely and securely deleted by the service provider across all regions.

Certification of cloud service providers

In terms of audit obligations, Insurance Europe would be supportive of allowing a system whereby cloud service providers can obtain certification that verifies certain quality standards and compliance with current regulations. Cloud providers that have been certified in such a way could also then be listed in a public register serving as an easy-to-access source of information. Service Organisation Control (SOC) reports could be used by regulators, for example, to provide evidence of compliance with relevant quality standards and/or regulations. Such reports are widely used within the industry and contain valuable information to assess and address the risks associated with an outsourced service.

Insurance Europe welcomes the ongoing work at European level on cloud security certification in order to enhance legal certainty and trust in the cloud market. The development of such a certification scheme will facilitate cloud uptake by demonstrating the equivalence of security requirements throughout Europe and making it easier to compare cloud service providers with respect to security when considering switching provider. It will also help to overcome the current patchwork of cloud security certification schemes. This will be of central significance for the further digitalisation of the industry.

Additional considerations

As regards further possible ways to address these challenges, it is important to ensure greater clarification of the legal responsibility and obligations of third-party providers vis-à-vis financial institutions and relevant

supervisory authorities. In this respect, it will be crucial to ensure an appropriate oversight framework of third-party providers by financial supervisory authorities. Insurance Europe therefore welcomes the general approach taken by the European Commission in its proposal for a Digital Operational Resilience Act to introduce a monitoring framework for critical ICT service providers in Europe. A harmonised and direct supervision of ICT service providers is an important step and should be accompanied by corresponding supervisory relief for financial institutions where relevant, which is currently not the case.

Insurance Europe also welcomes the planned approach by the European Commission to encourage and facilitate the development of standard contractual clauses for cloud outsourcing by financial institutions. The development of such model clauses would allow financial institutions to better reflect their sectoral regulatory constraints, eg Solvency II in the case of insurers, in their contractual agreements with cloud service providers.