SWIFT's response to the European Banking Authorities' consultation on "Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010"

SWIFT

01 August 2017

Confidentiality: Public

SWIFT thanks the European Banking Authority for the opportunity to provide comments on the consultation document "Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010".

SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholders, comprising more than 2,400 financial institutions. We connect more than 11,000 institutions in more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Natasha de Terán
SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467
www.swift.com

Patrick Krekels
SWIFT | General Counsel
Tel: + 32 2 655 3111
www.swift.com

We understand the EBA intends to issue guidelines and recommendations to competent authorities with a view to establish consistent, efficient and effective supervisory practises. We believe that EBA's recommendations to specify supervisory requirements and processes that apply when institutions are outsourcing to cloud service providers would be beneficial to the industry. Currently there is some uncertainty regarding the supervisory expectations that apply to outsourcing to cloud service providers, and there are also some differences in the national regulatory and supervisory frameworks for cloud outsourcing within the EU, for example on the type of services that are covered by guidelines on cloud outsourcing.

Cloud services versus outsourced cloud services

SWIFT believes it is important to explicitly state that these guidelines and recommendations ("guidelines") complement, and should therefore be read in conjunction with, the existing *CEBS Guidelines on outsourcing (CEBS guidelines).* In particular, it should be made clear that the guidelines only apply to outsourcing to cloud service providers when the outsourced service qualifies as "regulated outsourcing" under the applicable CEBS outsourcing guidelines.

In this respect, it is important to remind that cloud services should not all be considered as 'outsourced' services under the CEBS guidelines, which are subject to clearly defined criteria and exemptions. In some countries where regulators have issued specific guidelines on outsourcing to cloud providers, we have observed that some institutions have tended to apply these guidelines to *all* types of cloud services, without first applying the criteria and exemptions from the general outsourcing guidelines. To avoid the continuance of such confusion, we would suggest that all specific guidelines on cloud outsourcing should first restate the following criteria and exemptions which determine when a service may be considered as 'outsourced':

1. An activity that would normally be undertaken by the institution itself

The service must first of all be a service that an institution is able to perform itself, but decides to outsource for reasons of cost, efficiency, speed, etc. In other words, a service that an institution cannot perform on its own can therefore not be 'outsourced' to a service provider. Typical areas of services that institutions cannot perform on their own are services which benefit the industry at large, or a certain financial community, or which rely on, or seek to produce network effects. Examples of such include industry-wide financial communication networks, industry-wide databases with financial reference data, or industry-wide registries which contain, for instance, KYC or sanctions-related information, all of which may be performed as a cloud-based service.

2. A material activity

Secondly, the general outsourcing guidelines only apply to 'material' activities, ensuring there are no restrictions on institutions outsourcing non-material activities. The 2006 CEBS guidelines define 'material activities' as "(i) activities of such importance that any weakness or failure in the provision of these activities could have a significant effect on the authorised entity's ability to meet its regulatory responsibilities and/or continue in business; (ii) any other activities requiring a license from the supervisory authority, (iii) any activity having a significant impact on its risk management; and (iv) the management of risks related to those activities".

It is clear from the above definition that the concept of 'material' activities is limited to activities which, in case of failure, can have a direct impact on the ability of an institution to continue its business (such as accepting deposits, or lending). The definition does not include activities which simply provide tools or information which might assist the institution in performing its business independently and which do not outsource decisions or judgement calls to the service provider at any point in time. A typical area of such services assisting institutions in performing their business, without outsourcing the

decision-making, are services which provide institutions with financial business intelligence data or with information that might assist them in screening their clients or transactions against sanctions lists. The institutions remain in charge of making the decision as to which clients or transactions to authorise or not. Such services can be offered as a cloud-based service.

3. Exemption for standard services

Finally, the general outsourcing guidelines also confirm that 'standardised' products or services do not qualify as outsourced services. While it is clear that this exemption has covered services such as market information, price feed, or communication services (such as fax, phone, email, financial messaging) in the past, it has been less clear how the exemption applies to cloud services. Many such cloud services are fully standardised as well and should benefit from the same exemption. For instance, institutions will use third party connectivity services to host their websites or applications, while remaining in full control of the content of their communications.

There is a need to clearly define the scope of additional guidelines on outsourcing to cloud service providers. In order to avoid institutions applying such guidelines to all cloud services, without consideration as to whether they are material, standard, or capable of being undertaken by the institution itself, we believe it is important to restate the criteria and exemptions from the general outsourcing guidelines, and illustrate how they remain relevant to certain cloud services.

Relevance of equivalent arrangements

SWIFT understands the EBA is proposing that outsourcing institutions ensure they have agreements with cloud service providers in place and in writing. Further the EBA proposes that such agreements should stipulate that the cloud service providers undertake the obligation to allow access to its business premises and gives unrestricted rights to inspection and auditing by the outsourcing institutions.

While we understand the EBA's overarching intent with this proposal, we believe that these measures are redundant where alternative existing arrangements are already in place, which serve the same purpose and meet the same objectives as the recommendations set out in this proposal. We therefore believe concrete reference should be made to existing Union legal acts or other agreements and arrangements in place between cloud service providers and competent authorities which already contain requirements concerning the security of systems or data. Furthermore, if such existing requirements are *at least* equivalent to the obligations contained in the recommendations, we believe that those requirements should be an acceptable equivalent to the obligations, and that this should be explicitly stated in the recommendations.

One-stop shop mechanism

In the event that no such equivalent arrangements are in place, we believe that a single authority should be vested with access and audit rights on the cloud service provider.

We suggest that the cloud service provider should only ever be subject to its home Member State's competent authority only. Otherwise a cloud service provider with a presence in more than one Member State (e.g. via branches) could be subject to access and audit rights of several competent authorities making the execution of these controls overly burdensome for the provider and inefficient for the authorities concerned.

---------- END OF DOCUMENT ----------