New CSSF circulars on IT outsourcing

29 May 2017

In brief

On 17 May 2017, the *Commission de Surveillance du Secteur Financier* (CSSF) published four new circulars concerning IT outsourcing. These circulars both replace existing regulatory requirements specified in existing circulars, and introduce new matters, such as IT outsourcing based on cloud computing infrastructure.

These new regulatory requirements have the potential to change the design of the operational processes of regulated entities in Luxembourg, as well as redefining the landscape of IT service providers.

In detail

On 17 May 2017, The CSSF published four new circulars concerning IT outsourcing:

- Circular 17/654 on IT outsourcing based on cloud computing infrastructure;
- Circular 17/655 amending sections of CSSF Circular 12/552 on central administration, internal governance and risk management;
- Circular 17/656 replacing CSSF Circular 05/178 on IT outsourcing; and
- Circular 17/657 amending sections of CSSF Circular 06/240 on IT outsourcing and services provided under the status of support PSF.

Below, we have summarised the main changes introduced by these circulars:

IT outsourcing based on cloud computing infrastructure

Until CSSF Circular 17/654 was published, there were no dedicated regulatory requirements for IT outsourcing set-ups that are based on cloud technology. The general consensus was that cloud solutions were generally not permitted due to doubts surrounding the protection of sensitive data (including client data) and the transparency of internal controls (except if fully operated by an IT PSF).

The new CSSF Circular 17/654 not only introduces specific descriptions of the different characteristics, service models and deployment modes, but also supports the implementation of cloud-based solutions, both for financial institutions as consumers of such solutions and for future providers of cloud technologies in Luxembourg.

pwc

Depending on the intended set-up and attribution of roles as defined by the Circular, requirements have been defined to ensure that consumers of cloud-based services appropriately manage the risks related to delegating these activities to a service provider. These requirements are aligned with existing outsourcing requirements and mainly relate to aspects including internal governance and oversight, risk management, business continuity, protecting sensitive data, and contractual agreements with service providers. The Circular introduces the role of a Cloud Officer, whose job is to support governance and oversight objectives.

Cloud solutions providers do not need to be regulated entities under CSSF supervision. However, the counterparty signing the contractual agreement with the provider must ensure that all regulatory requirements specified by the Circular are complied with.

IT Function : Security watch and patch management

As part of the requirements to ensure robustness, efficiency, coherence and integrity of their IT Function, Credit Institutions (as well as Investment Firms) will need to implement a Security watch process to be informed as fast as possible about vulnerabilities, and are required to formalise procedures regarding the implementation of related security patches.

Compliance with these requirements implies to have technical knowledge to determine what are the real risks, but also a strong governance to take the best decision in sometimes short time frames.

How confidential client data is treated during IT outsourcing

CSSF Circular 12/552, as amended, introduced the concept of explicit client consent, which enabled credit institutions bound by professional secrecy obligations to outsource client-identifying data outside of Luxembourg. This client consent had to be based on an informed opinion regarding the purpose and nature of the outsourcing, as well as the concerned data, its location and recipient.

The new Circulars now additionally provide for client-identifying data to be processed outside of Luxembourg based on mere notification by the client(s) concerned. However, it is the obligation of the financial institution to assess the legal risks stemming from such an approach in order to conclude whether client notification for such data processing is sufficient or client consent is required.

The concept of client notification is currently also referred to in Bill no. 7024, which has not yet entered into force.

Besides, credit institutions are supposed to respect the applicable personal data protection regulation in such context.

Choice of service providers located outside of Luxembourg

CSSF Circular 12/552, as amended, provided the possibility to outsource IT operations abroad. However, such a set-up was only permitted if the financial institution outsourced to an entity of the group to which the financial institution belonged.

CSSF Circular 17/655 increases the scope of potential service providers abroad, as it permits any kind of IT service provider, including group-related ones, to operate an IT system. Similar limitations exists, in particular the requirements regarding client confidential data as described above.

Outsourcing requirements aligned between credit institutions and other regulated entities

In the past, credit institutions and investment firms had to comply with the IT outsourcing requirements specified in CSSF Circular 12/552, as amended, whereas specialist and support PSF service providers, as well as e-money and payment institutions, had to follow the requirements of CSSF Circular 05/178. The respective requirements were structured rather differently, and were limited to IT outsourcing in the case of CSSF Circular 05/178.

The new CSSF Circular 17/656, which applies to specialist and support PSF service providers, as well as e-money and payment institutions, is now much more closely aligned with the requirements of CSSF Circular 12/552, as amended, as sections concerning general outsourcing requirements and types of IT outsourcing and related requirements are identical in both circulars.

How can we help you?

Change means opportunity

The introduction of these new Circulars should be seen as an opportunity to reconsider current business models and operational processes in order to achieve your strategic objectives.

Our dedicated team of experts can help you to better understand the implications of these new regulatory requirements and to jointly explore possibilities to seize existing opportunities.

Subscribe to our Flash News on
www.pwc.lu/subscribe

Let's talk

Olivier Carré	Partner	+352 49 48 48 4174	olivier.carre@lu.pwc.com
Vincent Villers	Partner	+352 49 48 48 2367	vincent.villers@lu.pwc.com
Florian Bewig	Director	+352 49 48 48 4169	florian.bewig@lu.pwc.com

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with 2,700 people employed from 58 different countries. PwC Luxembourg provides audit, tax and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The helps its clients create the value they are looking for by giving comfort to the capital markets and providing advice through an industry-focused approach.
The PwC global network is the largest provider of professional services in the audit, tax and management consultancy sectors. We're a network of independent firms based in 157 countries and employing more than 223,000 people. Talk to us about your concerns and find out more by visiting us at www.pwc.com and www.pwc.lu.

© 2017 PricewaterhouseCoopers, Société coopérative. All rights reserved. In this document, "PwC Luxembourg" refers to PricewaterhouseCoopers, Société coopérative which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. PwC IL cannot be held liable in any way for the acts or omissions of its member firms.