New financial regulatory framework for outsourcing and specific rules for cloud services

June 09 2017 | Contributed by NautaDutilh Avocats Luxembourg Sàrl

AUTHORS

Jad Nader

Vincent Wellens

Introduction

On May 17 2017 the Luxembourg financial sector regulator (CSSF) published the following circulars in order to streamline its regulation of IT outsourcing in the financial sector and introduce specific rules for the use of cloud services:

- Circular CSSF 17/654 regarding IT outsourcing that relies on cloud computing infrastructure;
- Circular CSSF 17/655, which updated the outsourcing provisions in Circular CSSF 12/552 on the central administration, internal governance and risk management applicable to credit institutions and investment firms;
- Circular CSSF 17/656 on outsourcing by other financial service providers, payment institutions and e-money institutions, which aligned the rules set out in the now repealed Circular CSSF 05/178 with Circular CSSF 12/552's outsourcing provisions and the specific rules on outsourcing by authorised support financial service providers; and
- Circular CSSF 17/657, which updated Circular CSSF 06/240 on administrative and accounting organisation (ie, by adopting the concept of 'operation of IT systems' in order to exclude cloud-based services) and amended the IT outsourcing conditions that apply to branches located abroad.

Through these circulars, the CSSF has defined the conditions under which financial service providers may outsource activities, particularly IT-related activities, without infringing the regulatory principles of central administration and sound governance. These circulars complement the imminent legislative changes which will introduce an explicit legal exemption from the professional secrecy obligation applicable to the financial sector with regard to outsourcing.

Outsourcing in general

The Financial Sector Act 1993 sets out the regulatory principles of central administration and internal governance in the financial sector at a high level.

In Circular CSSF 12/552 (repealed and replaced by Circular CSSF 17/656), the CSSF provided a more detailed framework with respect to outsourcing, which particularly targeted IT outsourcing.

Circulars CSSF 12/552 and CSSF 17/656 contain several similar key elements, such as the need for:

- outsourcing to be:
  - consistent with a pre-defined policy based on a risk assessment; and
  - formalised in an agreement, including with regard to the service levels and specifications; and
- the outsourcing financial institution to control all stages of the outsourcing process.

Both circulars contain important restrictions on outsourcing activities that take place outside Luxembourg to the extent that they involve the processing of confidential data. For operations that involve a potential disclosure of confidential data, the outsourcing should be carried out by a so-called financial sector 'IT systems operator' within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act. These entities (often belonging to major IT groups) need prior authorisation in this respect and are supervised by the CSSF.

Circular CSSF 05/178 was particularly restrictive with regard to cross-border outsourcing, limiting such operations to certain types of intra-group outsourcing. Circular CSSF 12/552 is more liberal in this respect and allows intra and extra-group outsourcing to some extent – notably, when confidential data is encrypted and the decryption can take place only in Luxembourg. Further, Circular CSSF 12/552 allows outsourcing operations involving a potential disclosure of confidential data if the clients of the financial institution consent thereto.

Circular CSSF 17/655 updated Circular CSSF 12/552, which is applicable to credit institutions and investment firms as far as the outsourcing provisions are concerned.

Circular CSSF 17/656 repealed and replaced Circular CSSF 05/178 on outsourcing by financial service providers other than credit institutions and investment firms, as well as payment institutions and e-money institutions. It also aligned the obligations previously set out in Circular 05/178 with the outsourcing provisions set out in Circular CSSF 12/552, as amended by Circular CSSF 17/655.

In principle, Circulars CSSF 17/655 and 17/656 make the following changes to the outsourcing provisions set out in Circular CSSF 12/552:

- The requirement that the encryption key be in Luxembourg has been deleted.
- The obligation to base an outsourcing (involving the disclosure of confidential data) on client consent has been removed. As this obligation will be introduced to the Financial Sector Act as a legal exception to the professional secrecy obligation (the so-called 'banking secrecy' obligation) for outsourcing operations in the near future, there is no need to repeat this obligation in a circular (it being understood that the financial institution should nonetheless check whether it needs to inform its clients or obtain their consent under the Financial Sector Act).
- Certain additions have been made, such as the introduction of the principle that access to confidential data must take place in accordance with the principles of 'need to know' and 'least privilege'.

Further, Circular CSSF 17/656 contains specific rules for activities that authorised support financial service providers within the meaning of Articles 29-1 to 29-6 of the Financial Sector Act (which includes authorised IT system operators) outsource to another entity. The circular governs the following outsourcing situations:

- the use of infrastructures belonging to the group;
- the outsourcing of information technology for internal purposes to a third-party service provider; and
- the outsourcing by branches located abroad to local service providers.

These support financial service providers must obtain prior approval from their clients (ie, regulated entities) if the outsourcing concerns information that falls within the ambit of the client's professional secrecy obligation.

Circular CSSF 17/654 on use of cloud services

The CSSF adopted the so-called 'cloud circular', which deals specifically with financial institutions' use of cloud services. The cloud circular is applicable to every outsourcing scheme that meets the traditional definition of 'cloud computing' set out by the National Institute of Standards and Technology (ie, on demand self services and broad network access, resource pooling, rapid elasticity and measured services), on the condition that:

- the cloud computing service provider's employees cannot access data and systems held by the financial institution in the cloud without:
    - the financial institution's prior and express authorisation; and
    - the existence of a system to monitor such access being made available to the financial institution (such access must remain exceptional); and
- the cloud computing services do not involve the manual interaction of the cloud service provider in the daily management of the cloud computing resources used by the financial institution.

To the extent that the cloud circular is applicable, the outsourcing provisions in Circulars CSSF 17/655 and CSSF 17/656 will not apply.

The cloud circular contains the following obligations, among others.

If the operation of cloud resources (ie, the management of cloud resources via the client's interface) is not conducted by the client itself or has not been entrusted to a financial sector IT systems operator within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act, the client must proceed with a detailed risk analysis regarding the cloud service provider's activities, including – in particular:

- the roles and responsibilities (R&R) matrix between the operator and the cloud service provider;
- the management of client segregation; and
- audit rights on the part of the outsourcing entity.

The cloud circular contains several requirements on the governance of cloud services, including the following:

- A cloud officer must be appointed by the cloud resources operating entity (ie, the client or a third-party service provider).
- There must be a client-operator IT policy (if the latter is an external provider).
- The outsourcing must be done in accordance with a written outsourcing policy that has been approved by the authorised management (including an emergency and exit strategy).
- A R&R matrix and the means of communication must be documented, together with the cloud service provider's obligation to provide information regarding any significant problems impacting the outsourced activities.
- The client must understand and the operator (either the client or an external provider) must be able to control the cloud computing-related risks, such as:
    - the lack of segregation on a multi-tenant infrastructure;
    - the laws and regulations of the countries where data is stored;
    - the impact of the failure of a telecom network or service;
    - the use of the cloud as a shadow IT system; and
    - the lack of system/data portability.

The regulated entity must assess whether its clients must be informed or give their approval.

Depending on the materiality of the activity supported by the cloud infrastructure, the regulated entity must obtain prior approval from the CSSF. If such activities are not material or the cloud service contract is signed with a financial sector IT systems operator within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act, a simple notification to the CSSF is sufficient.

With regard to the management of risks relating to cloud-based outsourcing:

- the entity (ie, the client or external service provider) must have sufficient expertise with respect to this type of outsourcing to control the outsourced activities and manage the associated risks effectively. Further, there must be sufficient internal knowledge about the impact of the use of a software as a service (SaaS) programme;
- a prior and detailed analysis must be undertaken with regard to:
    - whether the outsourcing is in line with the principle of central administration;
    - the risks of hosting systems and data abroad;

    - the importance of the supported activities;
    - any vendor lock-in effect; and
    - the risks relating to chains of cloud-based outsourcing;
- there must be coherence between the information system security policies of the client (ie, the regulated entity), the operator (if different) and the cloud service provider; and
- changes in functionalities must be notified to the signatory of the cloud services contract before its implementation (the signatory can be the operator or the client).

With regard to the continuity of services:

- the client must be able to continue its critical activities in the event of exceptional circumstances or crises, even when it is subject to a winding-up or liquidation procedure; and
- the client and the signatory of the cloud services contract must ensure that the transfer of the cloud-based outsourced services can be insourced or transferred to another operator whenever the quality of the services risks being compromised.

With regard to system security:

- the confidentiality and integrity of the data and systems must be guaranteed throughout the whole IT outsourcing chain, whereby access to data and systems must take place in accordance with the principles of 'need to know' and 'least privilege';
- IT links must allow for rapid and unlimited access to stored information; and
- the operator must obtain information about the security measures implemented by the cloud services provider and ensure that their configuration is in line with the client's security policy.

With regard to contract clauses:

- the law applicable to the cloud services contract must be the law of an EU member state (exemptions can be requested from the CSSF for SaaS services);
- a resilience of data and systems within the European Union must be contractually foreseen (exemptions can be requested from the CSSF for SaaS services);
- a contract must be in place between the client and the operator (if applicable);
- qualitative and quantitative service levels must be provided;
- on the termination of the cloud services contract, the cloud service provider must delete the data and systems within a reasonable timeframe; and
- audit rights for the CSSF and the signatory of the cloud services contract must be granted.

With regard to the control of activities:

- it must be undertaken by way of key performance indicator measuring;
- the segregation of client data and systems must be controlled, including with respect to multi-tenant infrastructures; and
- the client's internal control function must have access to the data and systems hosted on the cloud infrastructure.

Audit rights include the right to access and review audit and certification reports. If necessary, the inclusion of non-covered elements must be foreseen contractually. In addition, there must be a collective or individual audit of processes, systems, premises, data and infrastructure to the extent that they are not covered in the audit or certification reports.

Circular CSSF 17/657 updates Circular CSSF 06/240 on administrative and accounting organisation in order to carve out cloud services from the 'operation of IT systems' concept, which – if offered by a Luxembourg entity to financial services providers – requires a specific authorisation under the Financial Sector Act. The question could be raised as to whether such exemption should be set out in the Financial Sector Act instead, given that an exemption to a provision of the latter can be adopted only by law and not via CSSF circulars.

Comment

The CSSF's new regulatory outsourcing framework accommodates the high demand among financial

institutions to outsource activities, especially in the IT field, as it provides more possibilities to do so and to use standard cloud services. However, where outsourcing is possible, it remains subject to strict conditions and under the CSSF's control.

In addition, some regulatory questions remain, such as the relationship between the new circulars and existing circulars – in particular, Circular CSSF 13/554 on the use and control of IT resources and the management of access to these resources. When a multinational financial group, including a Luxembourg entity, wishes to use a general access tool for IT resources at the group level, Circular CSSF 13/554 requires the Luxembourg financial institution to submit a formal, detailed authorisation request to the CSSF, proving that it still has full control over the IT resources for which it is responsible. This circular will need to be complied with, in addition to the May 17 2017 circulars on outsourcing.

For further information on this topic please contact Jad Nader or Vincent Wellens at NautaDutilh Avocats Luxembourg by telephone (+352 26 12 29 1) or email (jad.nader@nautadutilh.com or vincent.wellens@nautadutilh.com). The NautaDutilh Avocats Luxembourg website can be accessed at www.nautadutilh.com.
