In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 22 March 2006

To all credit institutions and other
professionals of the financial sector

CIRCULAR CSSF 06/240
as amended by Circulars CSSF 13/568 and CSSF 17/657

Re: Administrative and accounting organisation; IT outsourcing and details regarding services provided under the status of support PFS, Articles 29-1, 29-2, 29-3, 29-4, 29-5 and 29-6 of the Law of 5 April 1993 on the financial sector as amended (LFS)

Ladies and Gentlemen,

The purpose of this circular is to provide details on the implementation of Article 5(2) of the Law of 5 April 1993 on the financial sector as amended ("the Law") for banks and of Article 17(2) for professionals of the financial sector (PFS) when a financial professional relies on a third party for services likely to be subject to an authorisation as support PFS, in accordance with Articles 29-1, 29-2, 29-3, 29-4, 29-5 and 29-6 of the Law.

The details concern:

- the responsibilities of the financial professional as regards confidentiality when relying on a support PFS for services other than those requiring an authorisation;
- the differentiation between the status "IT systems and communication networks operator of the financial sector" ("OSIP" for Article 29-3 and "OSIS" for Article 29-4) as defined in Article 29-3 and 29-4 of the Law and the status "administrative agent" as defined in Article 29-2 of the Law;
- activities that require an authorisation as OSIP or OSIS;
- the proper use of interim staff for key IT functions;
- IT service provision, as a complement to "Circulars CSSF 17/656[1] and CSSF 12/552"[2], for system and data migration and user assistance (help desk);

[1] Repeals and replaces Circular CSSF 05/178
[2] Circular CSSF 13/568

- mail management and customer assistance functions;

1. <u>The responsibilities of the financial professional as regards confidentiality when relying on a support PFS for services other than those requiring an authorisation</u>

   1.1. The financial professional may want to resort to service providers with a support PFS status for services other than those requiring an authorisation.

   Article 41(5) of the Law stipulates that the professional secrecy obligation shall not exist "… insofar as the information communicated to those professionals is provided in pursuance of a service contract falling within the ambit of one of the activities regulated by the abovementioned legal provisions, and provided that the information concerned is essential for the execution of the service contract in question.". For the financial professional it is hence important to know whether this absence of obligation applies to all services provided by PFS as defined in Articles 29-1, 29-2, 29-3, 29-4, 29-5 and 29-6 of the Law, i.e. if it can entrust these service providers with activities subject to professional secrecy other than the activities linked to the operation of IT systems or communication networks.

   Considering that Articles 29-3(2) and 29-4(2) state that "IT systems operators … are entitled to install and maintain the IT systems …", and in order to avoid any ambiguity for the financial professional as regards professional secrecy in relation to the nature of the service provided, it should be clarified that the financial professional will not be bound by the obligation of professional secrecy for any service provided by a PFS with an OSIP or OSIS status.

   The financial professional relying on a support PFS is no longer required to ensure that the employees of the support PFS working on-site be constantly accompanied during their mission by an employee of the financial professional in charge of IT.

   1.2. While resorting to a support PFS is mandatory for activities requiring a licence, the financial professional may nevertheless freely opt for outsourcing other services with a support PFS. Where the financial professional opts for a support PFS, all services are provided within the legal and regulatory framework applicable to the financial sector. The financial professional may however not require the service providers to obtain a support PFS licence when they do not provide any service allowing them to obtain such an authorisation. A financial professional may thus not require his service provider to have an authorisation as OSIP or OSIS if the latter only provides locally software development or sale of equipment to the financial sector.

2. <u>Differentiation between the status "IT systems and communication networks operator of the financial sector" (OSIP or OSIS) and the status "administrative agent"</u>

This chapter describes how to identify a service provision that falls under the status of OSIP or OSIS or of administrative agent. Point 2.5. indicates the situations in which the administrative agent must cumulate the status of OSIP or OSIS.

2.1. Financial professionals subject to the conditions set out in Circular CSSF 17/656 "or Circular CSSF 12/552"[3] or Circular CSSF 17/654 on cloud computing shall ensure to conclude contracts in Luxembourg, for IT systems operation services (OSIP or OSIS) as defined in Chapter 3 of the present circular, with companies having an adequate authorisation.

2.2. In order to determine whether a service provision requires the status of OSIP or OSIS or administrative agent, the financial professional shall first evaluate if the activities to be outsourced exceed the purely technical provision of system operation services. If these services include tasks which may impact the financial professional's business, as for example the input of financial information an error of which could impact the business activity, the authorisation as OSIP or OSIS is not sufficient and the professional must refer to a company which is also authorised as administrative agent, as described under Article 29-2 of the Law.

2.3. The input/injection of data provided under the form of files by a third party or by the financial professional has to be considered as a technical task linked to the system interfaces as there is no human intervention by the service provider on the data. For instance, a file containing stock exchange prices or exchange rates may be input in the applications provided that the service provider does not add any appreciation on the correctness of the prices or rates. For the service provisions to remain only of a technical nature, the data may only be modified by an IT process, agreed with the financial professional who has to understand the effects thereof, and not by manual intervention of the service provider.

2.4. The technical settings of systems or applications, as for example the allocation of access rights to users, may nevertheless be considered as falling only under the status of OSIP or OSIS, provided that the definition of the access rights be controlled by the financial professional.

2.5. A financial professional may enter into an agreement with an administrative agent for the outsourcing of a series of activities supported by IT. As long as the service provider does not directly make its IT platform available to the financial professional for services other than administrative services - in other words, the platform is only used by the service provider in the context of services provided as administrative agent, even if the financial professional has access to it - the provision of services does not constitute an operator activity requiring the status as OSIP or OSIS, but it only requires the status as administrative agent. Thus, an administrative agent authorised under Article 29-2 of the Law may also use cloud computing services within the meaning of Circular CSSF 17/654, provided that these cloud computing

[3] Circular CSSF 13/568

services are not directly provided to the financial professional outside the scope of the provision of administrative services. The administrative agent shall, however, comply with the provisions of Circular CSSF 17/654 on cloud computing, in its capacity as ISCR (institution supervised by the CSSF and consuming cloud computing resources). If, on the other hand, the service provider puts at the disposal of the financial professional an IT equipment which it manages, but which is not used for its activity as administrative agent, the status of OSIP or OSIS becomes mandatory as the service provision is no longer of the same nature.

3. Description of the outsourced technical service in order to determine if it requires an authorisation as OSIP or OSIS

3.1. Where a technical service is not part of IT outsourcing relying on a cloud computing infrastructure as defined in Circular CSSF 17/654, it will be considered as operating activity when:

3.1.1. The service provision relates to equipment located in a production environment, which includes office equipment consisting of workplaces and printing or storage servers

and when at least one of the following two criteria is met:

3.1.2. The responsibility for the proper working of this equipment or of an application running on it is explicitly set out in the agreement or the financial professional has actually lost control and knowledge of the equipment or application on which the service provider intervenes.

3.1.3. The service provider operates on this equipment or application without the financial professional being always aware of it. This is the case when a service provider has an uncontrolled remote access or when a service provider is physically present on the premises but his actions and interventions on the systems are not sufficiently monitored by the financial professional.

3.2. Where a technical service is part of IT outsourcing relying on a cloud computing infrastructure as defined in Circular CSSF 17/654, it shall be considered as operating activity when it complies with the definition of resource operation of Circular CSSF 17/654.

3.3. Activities which do not require an authorisation as OSIP or OSIS

3.3.1 Provision of cloud computing services within the meaning of Circular CSSF 17/654.

3.3.2. In general, a financial professional may resort to external employees who are not members of a support PFS staff to assist in tasks on its

production systems which could include confidential data[4]. The financial professional shall limit, as far as possible, the occasional access to confidential data really necessary to the performance of tasks and to make sure, through a signed document, that this personnel is aware of the obligation of professional secrecy to which he/she is subject in accordance with Article 41 of the Law whenever he/she is working for the bank. The financial professional shall inform these employees of the criminal proceedings incurred in case of failure to respect the obligation of secrecy.

3.3.3. The supply, installation and configuration of IT equipment do not require an authorisation as OSIP or OSIS, unless the provision of services includes a support which goes beyond the mere corrective or adaptive maintenance.

3.3.4. Applications programming, assistance, advice and maintenance do not require an authorisation either, provided however that the provision of services does not include a support function discharging the financial professional of the operating or administration tasks of the systems or of the applications supplied.

3.3.5. Equipment and applications monitoring does not require an authorisation as OSIP or OSIS if the financial professional intervenes, in accordance with the instructions given by the service provider, on the monitored systems and if the service provider never has the means to intervene on its own initiative.

3.4. The financial professional shall determine and subsequently verify for each IT service provision to outsource or which has already been outsourced if it falls under the system and network operator activity.

4. Interim services

4.1. For the purposes of this circular, interim services shall mean the supply by a service provider of personnel with specific competences and remunerated by the service provider. The service agreement is thus concluded between the financial professional and the service provider who supplies the qualified personnel. On the other hand, bringing together qualified persons in order to accomplish a temporary work for the financial professional is not considered as an interim service within the meaning of this circular if these qualified persons are hired and remunerated by the financial professional.

4.2. Where temporary staff is hired, the tasks to carry out shall be clearly defined by the financial professional and the responsibility of the service provider shall be limited to suggesting persons having the qualification defined in the agreement.

[4] Only production systems are supposed to contain confidential data. The development and test systems should not contain confidential data.

4.3. Temporary employees shall be considered by the financial professional as third parties within the meaning of Circulars CSSF 17/656 and CSSF 12/552.

4.4. A financial professional may resort to interim services, but shall ensure to keep sufficient knowledge and skills to secure the continuity of its activities, in particular where the financial professional systematically relies on temporary staff for key functions in IT activities linked to the production environment, mainly due to the potential risks of a knowledge dilution for the financial professional in the long-term, of a lower contribution to the development of a corporate culture specific to the financial professional and to the financial sector, and of a possible loss of responsibility by this staff.

4.5. The financial professional shall be cautious when IT tasks linked to resource operation within the meaning of Circular CSSF 17/654 on cloud computing, system, network or database administration entrusted to temporary staff are realised on production equipment and not on development or test environments. These functions often imply important responsibilities, particularly as they allow the persons in charge full manipulation of the systems managed or the unrestricted access to data stored in the databases, due to the full access rights granted to these persons to accomplish their mission.

4.6. It is essential for the financial professional not to be in a dependency situation towards the temporary staff when these administration functions on production systems are entrusted to them. The financial professional shall therefore ensure that the duration of this service provision is limited to the bare minimum, i.e. the time necessary for it to recruit the personnel in charge of taking over the functions realised by the temporary staff or to entrust the outsourcing of these functions to a PFS with an OSIP or OSIS status.

5. <u>System and data migration</u>

5.1. System migration projects should be distinguished from data migration projects.

5.1.1. <u>System migration projects</u>

Data within system migration projects, whether confidential or not, does not constitute the main element of the project. The personnel in charge of the migration has a specific expertise of the old or the new system.

Considering that migration of the data itself within this type of project implies little manual intervention as compared to automatic migration processes which are developed, and assuming that the access to confidential data is limited and similar to that of projects for the implementation of IT applications, the financial professional may apply the principle of Circular CSSF 17/656 "(included in Circular CSSF 12/225)"[5] which states that the service provider intervening in a

[5] Circular CSSF 13/568

production environment which may contain confidential data shall be constantly accompanied during its mission by an employee of the financial professional in charge of IT. There is hence no need to systematically resort to a support PFS for this type of mission.

5.1.2. Data migration projects

These services mainly concern data processing and imply human data manipulation, combined with an expertise of data. The best example is archiving and indexation of documents. Archiving implies most of the time a manipulation of physical documents in order to digitize them and indexation of documents requires know-how of the service provider on this indexed data.

In both cases, the service provider has to access large amount of data being processed and confidentiality becomes a particular stake which requires the resort to a support PFS, as the financial professional can only delegate tasks giving access to confidential client data to professionals which the law exempts from professional secrecy. As a consequence, the financial professional must resort to a support PFS for any data migration project including confidential data. The financial professional shall moreover evaluate whether the manipulation of this data, for instance indexation, can have direct consequences on its business activity. If so, the service provision must be entrusted to a PFS authorised as administrative agent or PSDC (Articles 29-5 and 29-6 of the LFS) for archiving with probative value. The OSIP or OSIS or client communication agent status which includes archiving services is not sufficient in this case.

6. User assistance (helpdesk)

6.1. There are two categories of user assistance: assistance without control taking and assistance with remote control or configuration.

6.2. The first category does not require an authorisation as OSIP or OSIS as the actions executed on the systems are realised by the financial professional's staff based on indications given by the service provider which does not have access to these systems.

6.3. The second category consists in assistance by the service provider with control taking or configuration of the financial professional's system. Under these conditions, the service provider can operate the system remotely and the activity falls under the OSIP or OSIS status or even under the status of administrative agent if the service provider is in a position to remotely modify data linked to the business activity of the financial professional. This is particularly the case for the helpdesk function of a banking application, where the service provider takes remotely control over the screen of the financial professional's employees requesting assistance. On the one hand, the presence of the assisted person is no longer required once the session has

been initiated; on the other hand, the service provider has control over the application in the name of the assisted person and may modify the current transaction, or even input new ones. In addition to the confidentiality issue raised by this distance viewing, there is a risk of interference in the activities of the financial professional by the service provider, including the underlying risks for error or fraud.

6.4. Assistance with remote control, by a cloud provider within the meaning of Circular CSSF 17/654 is only allowed as support and under the control of the resource operator and not directly to the ISCR[6]. Indeed, the resource operator is the guarantor of the operation made for the ISCR.

7. Mail management and client assistance (helpdesk)

7.1. Where a financial professional outsources its incoming or outgoing mail management or where it uses an external service provider for a client assistance service (call centre or helpdesk), the risk incurred for disclosure of clients' identity is high and it is essential for the service provider to maintain secrecy of the information obtained. Pursuant to Article 41(5), the financial professional has no right to entrust a service provider with tasks giving access to confidential data if the latter is not authorised as a support PFS and in particular as client communication agent.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT Director	Jean-Nicolas SCHAUS Director General

[6] Within the meaning of Circular CSSF 17/654.