Commission de Surveillance du Secteur Financier

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

Luxembourg, 17 May 2017

To all credit institutions and PFS[1]
To all payment institutions and electronic money institutions[2]
To all investment fund managers[3]

CIRCULAR CSSF 17/654 as amended by Circular CSSF 19/714

Re: IT outsourcing relying on a cloud computing infrastructure

Ladies and Gentlemen,

The purpose of this circular is to clarify the regulatory framework governing IT outsourcing relying on a cloud computing infrastructure (hereafter also "cloud computing solution") provided by an external provider. The use of a private cloud without outsourcing is thus excluded from the scope of this circular.

This circular applies to:

- all credit institutions and PFS within the meaning of the Law of 5 April 1993 on the financial sector ("LFS");
- all payment institutions and electronic money institutions within the meaning of the Law of 10 November 2009 on payment services ("LPS");
- all investment fund managers subject to Circular CSSF 18/698.

[1] Authorised under the Law of 5 April 1993 on the financial sector ("LFS").
[2] Authorised under the Law of 10 November 2009 on payment services ("LPS").
[3] Subject to Circular CSSF 18/698.

This circular contributes to the sound and prudent management, the proper organisation of these entities and the preservation of information security of these entities[4].

This circular defines:

- "cloud computing";
- the requirements with respect to outsourcing to a cloud computing infrastructure.

The instructions to inform the CSSF of the outsourcing to a cloud computing infrastructure in accordance with the requirements of paragraph 26 of this circular are available on the CSSF website[5].

I. Definitions

a. Specific vocabulary

1. "Institution" shall mean a legal person.

1a. "Competent authority" shall mean the CSSF or the European Central Bank for Luxembourg credit institutions falling under its supervision.

2. "ISCR" shall mean an institution supervised by the competent authority and consuming cloud computing resources for the purpose of carrying out its activities.

3. "Cloud computing resource" shall mean any computing capabilities (e.g. server, storage, network, etc.) provided by a cloud computing service provider.

4. "Cloud computing service provider" shall mean any firm proposing cloud services within the meaning of the definition of this circular.

5. "Outsourcing" shall mean the complete or partial transfer of the operational functions, activities or services of the institution to an external service provider, which is part of the group to which the institution belongs or not.

6. "Multi-tenant" shall mean a physical or logical infrastructure serving several ISCRs through shared cloud computing resources and by means of a standardised model.

[4] As required, inter alia, under Article 5(1a) of the LFS, Article 17 of the LFS and Article 11(2) of the LPS, point 135 of Circular CSSF 18/698, Article 5(2) of CSSF Regulation N° 10-4 and Article 57(2) of Delegated Regulation (EU) 231/2013.

[5] Link: https://www.cssf.lu/en/ict-risk/

7. "Client interface" shall mean the software layer made available by the cloud computing service provider to the ISCR allowing the latter to manage its cloud computing resources.

8. "Resource operation" shall mean managing cloud computing resources made available through the client interface. By extension, "resource operator" shall mean the natural or legal person that uses the client interface to manage the cloud computing resources.

9. "Signatory" shall mean the institution that signs the contract with the cloud computing service provider.

10. "Material activity" shall mean any activity that, when it is not carried out in accordance with the rules, reduces the institution's ability to meet the regulatory requirements or to continue its operations as well as any activity necessary for sound and prudent risk management.

b. Definition of "cloud computing"

11. Using a cloud computing solution is considered as outsourcing. In order to define cloud computing and distinguish it from traditional outsourcing, the CSSF relies on the definitions proposed by international organisations[6].

12. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models, as presented subsequently in paragraphs 14, 15 and 16.

13. The cloud computing infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually, the abstraction layer sits above the physical layer.

14. The five essential characteristics that define the concept of cloud computing are:

[6] The National Institute of Standards and Technology (NIST) or the European Union Agency for Network and Information Security (ENISA).

a. On-demand self-service: An ISCR[7] can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with the cloud computing service provider.
b. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin (e.g. browsers) or thick client (e.g. specific applications) platforms (e.g. mobile phones, tablets, laptops and workstations).
c. Resource pooling: The cloud computing service provider's computing resources are pooled to serve multiple ISCRs using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to ISCR demand. There is a sense of location independence in that the ISCR generally has no control or knowledge over the exact location of the provided resources, but may be able to specify the location at a higher level of abstraction (e.g. country, region or data centre). Examples of resources include storage, processing, memory and network bandwidth.
d. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the ISCR, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
e. Measured service: Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and the ISCR of the utilised service.

15. Cloud computing service providers usually propose three service models:
a. Infrastructure as a Service (IaaS): The capability provided to the ISCR is to provision processing, storage, networks and other fundamental computing resources where the ISCR is able to deploy and run arbitrary software, which can include operating systems and applications. The ISCR does not manage or control the underlying cloud computing infrastructure, but has control over operating systems, storage and deployed applications, and possibly limited control of select networking components (e.g. host firewalls).
b. Platform as a Service (PaaS): The capability provided to the ISCR is to deploy onto the cloud computing infrastructure ISCR-created or acquired applications or applications created using programming languages, libraries, services and tools supported by the provider (this functionality does not prevent the use of programming languages, services and tools from other sources). The ISCR does not manage or control the underlying cloud computing infrastructure, including network, servers, operating systems or

[7] For the sake of clarity, the definition considers the case where the ISCR itself is the operator of the resources used.

storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

c. Software as a Service (SaaS): The capability provided to the ISCR is to use the provider's applications running on a cloud computing infrastructure. These applications are accessible from various client devices through either a thin client interface, such as a web browser, or a programme interface. The ISCR does not manage or control the underlying cloud computing infrastructure, including network, servers, operating systems or storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

16. In addition, four cloud computing deployment models are generally used:
    a. Private cloud: The cloud computing infrastructure is provisioned for exclusive use by a single organisation or by multiple entities of the same group. It may be owned, managed and operated by the institution, a third party (including an entity of the group to which the institution belongs) or some combination of them, and it may exist on or off premises.
    b. Community cloud: The cloud computing infrastructure is provisioned for exclusive use by a specific community of ISCRs from institutions that have shared concerns (e.g. mission, security requirements, policy and compliance considerations). It may be owned, managed or operated by one or more of the ISCRs in the community, a third party, or some combination of them, and it may exist on or off the ISCRs' premises.
    c. Public cloud: The cloud computing infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organisation, or some combination of them. It exists on the premises of the cloud provider.
    d. Hybrid cloud: The cloud computing infrastructure is a composition of two or more distinct cloud computing infrastructures (private, community or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

c. Applicability of the circular

17. An outsourcing is considered as "outsourcing to a cloud computing infrastructure" within the meaning of this circular and governed by the requirements of this circular if the five essential characteristics defined in paragraph 14 and both of the following specific requirements are fulfilled:
    a. Under no circumstances may staff employed by the cloud computing service provider access data and systems that an ISCR owns on a cloud computing infrastructure without prior and explicit agreement of the ISCR and without monitoring mechanism available to the ISCR to control the accesses. These accesses must remain exceptional. Under other circumstances, access may be necessary under a legal requirement or in an extreme emergency following a

critical incident affecting part of or all the ISCRs of the cloud computing service provider[8]. All accesses of the cloud computing service provider must be restricted and subject to preventive and detective measures in line with sound security practices and audited at least annually.

b. The cloud service provision does not entail any manual interaction by the cloud computing service provider as regards the day-to-day management of the cloud computing resources used by the ISCR[9] (e.g. provisioning, configuration or release of cloud computing resources). Thus, the resource operator alone (i.e. either the ISCR or a third party other than the cloud computing service provider) shall manage its IT environment hosted on the cloud computing infrastructure. However, the cloud computing service provider may intervene manually:
    - for global management of IT systems supporting the cloud computing infrastructure (e.g. maintenance of physical equipment, deployment of new non ISCR-specific solutions); or
    - within the context of a specific request by the ISCR (e.g. provisioning of a cloud computing resource that is missing in the catalogue proposed by the cloud computing service provider or performing insufficiently).

18. IT outsourcings fulfilling these seven conditions (defined in paragraphs 14 and 17) shall no longer be subject to Circular CSSF 17/656[10], to Sub-chapter 7.4 of Circular CSSF 12/552 or to the provisions related to outsourcing of Section 5.1.2 and to Sub-chapter 6.2 of Circular CSSF 18/698. IT outsourcings that do not fulfil all of these conditions remain subject to Circular CSSF 17/656, to Sub-chapter 7.4 of Circular CSSF 12/552 or to the provisions related to outsourcing of Section 5.1.2 and to Sub-chapter 6.2 of Circular CSSF 18/698, as the case may be.

II. Requirements to be observed with respect to outsourcing to a cloud computing infrastructure

19. The requirements below shall apply to the whole outsourcing chain as soon as all outsourced services are purely IT in nature and at least one of the outsourcing services meets the definition of cloud computing within the meaning of this circular. Thus, the requirements of this circular do not apply to business process outsourcing, even if this kind of outsourcing relies itself on an outsourced cloud computing infrastructure.

[8] In cases of extreme emergency, the ISCR should be informed a posteriori.
[9] Indeed, it is an automated system that allows provisioning resources, hence point (a) specifying that staff may not have access by default to ISCR resources.
[10] Circular CSSF 17/656 repeals and replaces circular CSSF 05/178.

19a. Proportionality[11] shall apply to the implementing measures which institutions take pursuant to this circular having regard to the nature, scale and complexity of the activity outsourced to a cloud computing infrastructure, including the risks. Thus, pursuant to the principle of proportionality, the ISCR may justify not applying the requirements set out in the following paragraphs of this circular where only non-material activities are outsourced to a cloud computing infrastructure and in accordance with its risk analysis.

- 27.j: notification by the cloud computing service provider in case of change of functionalities;
- 27.k: notification by the resource operator in case of change of functionalities;
- 28.b: continuity in case of resolution or reorganisation or another procedure;
- 28.c: transfer of services in case the continuity is threatened;
- 30: monitoring of activities;
- 31.a: contract under the European Union law;
- 31.b: resiliency of the services in the European Union;
- 31.j: right of audit for the ISCR;
- 32: details regarding the right of audit;
- 33: exercise of the right of audit.

20. Several cases should be distinguished to identify the signatory of a cloud computing service contract:
    a. Where the ISCR itself is the resource operator, the service contract is signed between the ISCR and the cloud computing service provider (the signatory is the ISCR).
    b. Where a third party is in charge of resource operation, the contract shall be signed:
        - either between the ISCR and the cloud computing service provider (the signatory is the ISCR); or
        - between the resource operator and the cloud computing service provider (the signatory is the resource operator).

21. Where the signatory is not the ISCR and not subject to the supervision of the competent authority, the ISCR subject to this circular is required to ensure that the signatory fulfils the requirements set out therein.

22. It should be noted that an ISCR relying on an institution that cumulates the activities of "cloud computing service provider" and "resource operator" is subject to the requirements of this circular provided that both activities are properly segregated (i.e. so that staff exercising the "cloud computing service provider" function cannot access data and thereby continues to fulfil the

[11] In accordance with the principle of proportionality referred to in the CEBS guidelines on outsourcing of 14 December 2006 which were clarified by the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

definition of "cloud computing" within the meaning of this circular). The same is true where the institution cumulating both functions has been granted one of the authorisations defined in Articles 29-3 or 29-4 of the LFS. If this segregation requirement cannot be fulfilled, the requirements of Circular CSSF 17/656 or of Sub-chapter 7.4. of Circular CSSF 12/552 or the provisions related to outsourcing of Section 5.1.2and Sub-chapter 6.2 of Circular CSSF 18/698 remain applicable.

23. Resource operation:

The CSSF considers that the "resource operation" as defined in paragraph 8 shall be carried out:

a. by the institution that subscribed to a cloud computing offer. In such a case, the service contract is signed between the institution and the cloud computing service provider. The institution is thus the "signatory", the "ISCR" as well as the "resource operator"; or
b. by a third party (in such a case, the institution is the "ISCR" and the third party is the "resource operator"). A distinction must be made between two cases:
    - Resource operation is carried out by an institution authorised under Articles 29-3 or 29-4 of the LFS. In this case, the resource operator shall be able to justify, at a technical level, the operation of resources for ISCRs and shall have concluded with each ISCR at least a service contract pertaining to these resource operations. Moreover, the function of resource operator may only be sub-contracted to another institution having been granted an authorisation as defined in Articles 29-3 or 29-4 of the LFS and provided that the provision is complementary[12] and does not void the first institution of its operational substance. Indeed, these activities are considered as material for institutions authorised under Articles 29-3 or 29-4 of the LFS. These institutions shall also comply with the requirements of this circular where the operation of resources is carried out for an institution which is not subject to the supervision of the competent authority.
    - Resource operation is carried out by an institution that is not authorised under Articles 29-3 or 29-4 of the LFS, either because it is located abroad, or because it is an entity of the group to which the institution belongs and which provides operating services exclusively within the group. In such a case, in addition to complying with the requirements set out in this circular, the ISCR shall have made a thorough risk analysis of the activities of the resource operator, notably by verifying that the following points have been correctly addressed:
        – the roles and responsibilities defined between the resource operator and the cloud computing service provider;

[12] An example of complementarity is the operation of resources in SaaS mode by the first institution and the cascading operation of resources in IaaS mode of the underlying infrastructure by the second institution.

- the management of the isolation of multi-tenant environments;
- the indicators collected by the resource operator to monitor the systems and data on the cloud computing infrastructure;
- the technical and organisational security measures implemented to access the client interfaces in order to manage the cloud computing resources, including the management of client interface access;
- the consistency of the operations and security policies defined by the resource operator with the configurations of the cloud computing resources and the planned security measures;
- the competences of the operators (e.g. certifications, technical training);
- the review of the audit reports of the cloud computing service provider by the resource operator;
- the competent authority's and the ISCR's right to audit the resource operator (in line with the requirements described in points 31.i, 31.j and 32);
- the competent authority's, the ISCR's and the signatory's right to audit the cloud computing service provider (in line with the requirements described in points 31.i, 31.j and 32).

24. Governance:
   a. The use of cloud computing services shall not relieve the ISCR of its legal and regulatory obligations or of its responsibilities towards its clients. It shall not result in any delegation of the ISCR's responsibility to the cloud computing service provider or the resource operator.
   b. The final responsibility for the risk management associated with the use of cloud services is incumbent upon the ISCR which is proceeding to outsource to a cloud computing infrastructure. The ISCR shall designate among its employees one person who will be responsible for the management of the outsourcing relationship.
   c. The resource operator shall designate among its employees one person, the "cloud officer", who shall be responsible for the use of cloud services and shall guarantee the competences of the staff managing cloud computing resources (cf. point 27.a). The resource operator shall assign the function of "cloud officer" to a qualified person that masters the challenges of outsourcing to a cloud computing infrastructure. This function may be taken on by persons that already cumulate other functions within the IT department.
   d. If resource operation is performed by the ISCR, the "cloud officer" may cumulate the responsibility for the outsourcing relationship management as defined in point (b). If the ISCR relies on a third person for cloud computing resource operation, the ISCR must know the name of the "cloud officer" of the resource operator.
   e. The ISCR and the resource operator shall implement an IT policy that covers all IT activities spread out among the ISCR and all the actors in the

outsourcing chain. This policy shall take into account the means made available by the cloud computing service provider (e.g. security tools), while complying with the requirements of this circular. The IT organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the ISCR and the resource operator and the procedure manuals shall be adapted accordingly.

f. Any outsourcing of material or non-material activities to a cloud computing infrastructure, including that carried out within the groups to which the ISCR and the resource operator belong, shall be in line with a written outsourcing policy requiring approval from the authorised management and including the contingency plans and exit strategies. The authorised management shall reapprove and update on a regular basis the institution's outsourcing policy, while ensuring that appropriate changes are rapidly implemented. Any approval for outsourcing to a cloud computing infrastructure shall be the subject of an official and detailed contract.
g. The written documentation should also provide a clear description of the responsibilities of the parties as well as clear communication means accompanied by an obligation for the cloud computing service provider and the resource operator to report any significant problem having an impact on the activities outsourced to a cloud computing infrastructure as well as any emergency situation.
h. The ISCR and the resource operator shall have full awareness of the continuity and security elements remaining under their responsibilities when using a cloud computing solution.
i. The ISCR shall understand and the resource operator shall control the risks linked to a cloud computing infrastructure.
j. The ISCR and the resource operator shall know at any time where their data and systems are located globally[13], be it production environments or replications or backups.

25. Client notification and consent:
    a. The ISCR shall ensure protection of the data concerned by the outsourcing in accordance with the General Data Protection Regulation (GDPR) and with the requirements of the authority competent in this matter, the National Commission for Data Protection (CNPD);
    b. The ISCR shall apply the provisions of Article 41(2a) of the LFS with respect to professional secrecy.

26. Necessity to inform the competent authority (register, notification and authorisation):
    a. Any institution falling under the scope of this circular shall maintain a register of all cloud computing infrastructure outsourcing, whether the

[13] It is important that the ISCR and the resource operator know in which country data is stored, in a global way. For example, data is shared between country A and country B, but cannot be in country C under no circumstances.

outsourced activities are material or non-material. This register shall be transmitted to the competent authority upon request.

b. In case of use of a cloud computing infrastructure outsourcing for a material activity within the meaning of paragraph 10, the ISCR shall notify the competent authority if one of the following conditions is fulfilled:
   - The cloud computing service provider is an institution that is authorised under Articles 29-3 or 29-4 of the LFS and the resource operation is carried out either by the ISCR or by an institution authorised under Articles 29-3 or 29-4 of the LFS.
   - Resource operation is carried out by an institution authorised under Articles 29-3 or 29-4 of the LFS, where it is the signatory.

c. In case of use of a cloud computing infrastructure outsourcing for a material activity within the meaning of paragraph 10, the ISCR shall request prior authorisation from the competent authority if none of the conditions listed in point (b) are fulfilled.

d. An authorisation is still required in the particular case where an institution authorised under Articles 29-3 or 29-4 of the LFS acts as intermediary and not as resource operator between an ISCR and a cloud computing service provider.

e. In case of use of a cloud computing infrastructure outsourcing for a material activity within the meaning of paragraph 10, any institution subject to the supervision of the competent authority that wishes to terminate a cloud computing infrastructure outsourcing shall notify the competent authority of its decision.

f. For material activities, any institution subject to the supervision of the competent authority and intending to change its cloud computing service provider or models (as defined in paragraphs 15 and 16) or its resource operator shall inform anew the competent authority in accordance with the requirements of points 26.b to 26.d.

g. Any institution authorised under Articles 29-3 or 29-4 of the LFS shall request authorisation from the competent authority before marketing in the following cases:
   - The institution intends to outsource to a cloud computing infrastructure as a signatory to provide a resource operator service to its clients supervised by the competent authority.
   - The institution intends to provide a cloud computing infrastructure to its clients supervised by the competent authority, acting thus as a cloud computing service provider.
   - The institution intends to provide a cloud computing solution to its clients supervised by the competent authority by relying on one or more cloud computing infrastructures. The institution acts then as a sub-contracting cloud computing service provider.

h. The register, the notifications to the competent authority and the authorisation requests to the competent authority referred to in points 26.a

to 26.g shall be formalised by following the instructions available on the CSSF website[14].

27. Management of outsourcing risks:
    a. The resource operator shall retain the necessary expertise to effectively monitor the outsourced services or functions on a cloud computing infrastructure and manage the risks associated with the outsourcing. Moreover, the resource operator shall ensure that staff in charge of cloud computing resources management, including the "cloud officer", internal audit and the Information Security Officer have sufficient competences to take on their functions based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider. The "cloud officer" is in charge of implementing this requirement.
    b. In order to enable the ISCR to assess the reliability and completeness of the data produced by the IT system as well as its compatibility with the accounting and internal control requirements, there should be one person among its staff members with the necessary IT knowledge to understand both the impact of the programmes on the accounting system and the actions performed by the third party within the context of the provided services. The ISCR shall also have, in its premises, sufficient documentation on the programmes used.
    c. The ISCR that wishes to use a cloud computing service shall base its decision on prior and formalised analysis demonstrating that it does not result in the relocation of the central administration. This analysis shall include at least a detailed description of the services or activities to be outsourced to a cloud computing infrastructure, the expected results of the outsourcing and an evaluation of the risks of the outsourcing project as regards financial, operational, legal and reputational risks. These risks encompass, e.g.: isolation failure in multi-tenant environments, the various legislations that are applicable (country where data are stored and country where the cloud computing service provider is established), interception of data-in-transit, failure of telecommunications (e.g. Internet connection), the use of the cloud as "shadow IT"[15], the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of continuity of cloud computing services.
    d. Moreover, for an outsourcing to a cloud computing service provider abroad or hosting its systems abroad, the analysis shall notably take into consideration the geopolitical risks and the laws applicable in the foreign country, including the law on data protection, as well as the implementing provisions, notably those relating to insolvency in case of default of a cloud computing service provider.

[14] Link : https://www.cssf.lu/en/ict-risk/
[15] "Shadow IT" is the use of IT resources that is non-controlled by the IT department.

e. The ISCR and the resource operator shall pay special attention to the outsourcing to a cloud computing infrastructure of critical activities in respect of which the occurrence of a problem may have a significant impact on the ISCR's and resource operator's ability to meet the regulatory requirements or even to continue their activities.
f. The ISCR and the resource operator shall pay special attention to the concentration and dependence risks which may arise when large parts of their activities or important functions are outsourced to a single cloud computing service provider during a sustained period.
g. The ISCR and the signatory shall take into account the risks associated with chain outsourcing ("sub-outsourcing", where a cloud computing service provider outsources part of the activities to other service providers). In this respect, they shall pay special attention to the safeguarding of the integrity of the internal and external control.
h. The resource operator which has an authorisation under Articles 29-3 or 29-4 of the LFS and which is signatory, as well as the ISCR, shall take into account the impact of the outsourcing on the activities and risks in their policies as regards outsourcing. They shall make sure that the reporting provided as well as the control mechanisms implemented by the cloud computing service provider are in line with their policies. Outsourcing to a cloud computing infrastructure may, by no means, lead to the circumvention of any regulatory restrictions or prudential measures of the competent authority or challenge the competent authority's supervision.
i. The IT system security policies of the ISCR and of the resource operator shall take into account their cloud computing service providers' security measures made available to the ISCR and the resource operator in order to ensure overall consistency.
j. Any change in the application functionality by the cloud computing service provider - other than the changes relating to corrective maintenance - shall be communicated to the signatory, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity. Where the signatory is not the ISCR, the signatory shall inform the ISCR who is likely to be impacted by a change.
k. Any change in the application functionality managed by the resource operator - other than the changes relating to corrective maintenance - shall be communicated to the ISCR, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity.

28. Business continuity:
a. The ISCR shall be able to continue its critical functions in case of exceptional events or crisis.
b. The ISCR and the signatory shall take the necessary measures – contractual if necessary - to ensure continuity of the cloud computing services if one of them underwent resolution or reorganisation measures or winding-up proceedings or, where applicable, bankruptcy, controlled management,

suspension of payments, compositions and arrangements with creditors aimed at preventing bankruptcy or other similar proceedings.

c. The ISCR and the signatory shall also take the necessary measures to be in a position to adequately transfer the outsourced activities on a cloud computing infrastructure to a different provider or to perform those activities itself whenever the continuity or quality of the service provision are likely to be affected. As a consequence, the signatory shall be able, financially and operationally, to recover the data and systems of the ISCR, so that the ISCR can use the data and continue its activities. It should be noted that when using a software relying on a cloud computing infrastructure, the ISCR shall take into consideration the potential need to migrate to a software other than the one used.

d. The resource operator shall select and configure the cloud computing resources in compliance with the ISCR's continuity plan. It also provides for the regular control of backups and of the facilities to restore backups. Indeed, the use of cloud computing does not necessarily and by default guarantee the ISCR that the continuity solutions and backups it deemed necessary are available.

29. Systems security:

a. The confidentiality and integrity of data and systems must be controlled throughout the IT outsourcing chain. A level of protection that is adapted to the sensitivity of data is expected from all actors (the ISCR, the resource operator and the cloud computing service provider). In particular, access to data and systems shall follow the "need to know" and "least privilege" principles, i.e. access is only granted to persons whose functions require so, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.

b. The signatory and the ISCR shall ensure that sufficient protection measures are taken in order to avoid that non-authorised persons access their systems. The signatory and the ISCR shall, in particular, make sure that telecommunications are encrypted or protected through other available technical measures to ensure the security of the communication.

c. The signatory and the ISCR shall ensure that the network link allows a quick and unlimited access to the information stored in the processing unit (i.e. through an appropriate access path and data rate and through redundancy).

d. The resource operator shall inform itself about the security measures made available on the cloud computing infrastructure and ensure that the configuration is compliant with the security policy of the ISCR.

30. Monitoring of activities:

a. The cloud computing service provider shall provide regular indicators to the signatory. These indicators allow the signatory to efficiently follow the service quality and to note deviations from the contractually expected levels.

b. The signatory shall be able to provide relevant indicators to the ISCR.

c. The signatory shall have assurance that the controls operated by the cloud computing service provider are in line with the good practices and operate efficiently.
d. The isolation of the ISCR's systems and data shall be regularly controlled by the cloud computing service provider, notably by means of penetration tests performed by professionals with adequate skills.
e. At any time, isolation must be justified by the resource operators at the level of the multi-tenant environments of the ISCRs. At any time, the resource operator shall be able to demonstrate the proper isolation of the multi-tenant environments of its ISCR clients.
f. The internal control functions of the ISCR shall have adequate access to data and systems necessary to exercise their missions which are hosted on the cloud computing infrastructure.

31. Contractual clauses:
a. The service contract signed with the cloud computing service provider shall be subject to the law of one of the EU countries.
b. The service contract signed with the cloud computing service provider shall provide for a resiliency of the cloud computing services provided to the ISCR in the European Union. In this way, in case of spread of processing, data and systems over different data centres worldwide, at least one of the data centres shall be located in the European Union and shall, if necessary, allow taking over the shared processing, data and systems in order to operate autonomously the cloud computing services provided to the ISCR. If all data centres backing the cloud computing services are located within the European Union, the resiliency requirement for the cloud computing services in the European Union is by default fulfilled.
c. The ISCR may apply for a special derogation to the competent authority where the requirements laid down in points (a) and (b) above cannot be fulfilled in case of a material outsourcing. This application for derogation shall be supported by detailed arguments justifying the use of this cloud computing service provider and stating precisely the resilience measures planned in case of this provider's failure or failure of connections allowing access thereto.
d. Where the ISCR uses a third party for resource operation, a service contract between the ISCR and the resource operator must govern this outsourcing agreement. This contract shall provide for the right of the ISCR to audit the resource operator. If the signatory of the service contract with the cloud computing service provider is the resource operator, this contract shall include the necessary clauses (e.g. the possibility to transfer the information and the audit reports) so that the ISCR may efficiently control the outsourcing "chain".
e. The roles and responsibilities, shared among all the parties in the outsourcing chain (ISCR, resource operator and cloud computing service provider), shall be specified in the service contracts. The whole needs to remain consistent.

f. Every service contract, signed between the parties in the outsourcing chain (ISCR, resource operator and cloud computing service provider), shall clearly define the expected levels of services, qualitatively and quantitatively.
g. If the contract is terminated, the provider shall contractually commit to definitely erase the data and systems of the signatory within reasonable time frame without prejudice to legal provisions.
h. In the event of an incident, regulatory needs or other specific requirement, the signatory shall have an appropriate means of contact at the cloud computing service provider. The procedure for relating the parties shall be duly documented in the service contract.
i. The competent authority shall have an unconditional right of audit of resource operators and cloud computing service providers within the scope of the services used by an institution under its supervision where the outsourced activity is material, including for any relevant outsourcing chain which is directly linked to the provision of cloud computing services by the ISCR. The competent authority's right of audit shall be laid down contractually and comprise, among other things:
    - Access to the institution's data and systems hosted on a cloud computing infrastructure. This access shall be managed by the resource operator.
    - Access to the relevant documentation of the cloud computing service provider (this documentation shall notably include audit reports, certification reports, policies and procedures).
    - Access to the staff of the cloud computing service provider, subject to prior notification within a reasonable time frame.
    - The possibility to carry out on-site inspections.
    - The possibility to communicate observations to the supervised institution (ISCR and resource operator).
j. The service contract signed with the cloud computing service provider shall provide that the signatory keeps a right to audit the cloud computing service provider within the scope of the services used, as defined in paragraph 32. If the ISCR is not signatory and in accordance with point (d), the right of the ISCR to audit the cloud computing service provider shall be performed through the resource operator which is the signatory. In this case, the contract concluded between the ISCR and the resource operator shall provide that the ISCR can be mandated as auditor by the resource operator in order to perform its right of audit on the cloud computing service provider, as required under paragraph 33. This request to perform the right of audit shall be granted to the ISCR, which ensures the possibility for the ISCR to perform its right of audit at any time.

32. Right to audit:
    a. The signatory shall contractually retain the right to audit the cloud computing service provider. The right of audit guarantees to its beneficiary the right to access data related to the outsourced activities as well as the right to perform, on its own initiative and any time, an assessment of the cloud

computing service provider's processes, systems, networks, premises, data and infrastructure used for providing the services outsourced, including the parts of the services that may be sub-outsourced. The right to audit should not be subject to such conditions that its performance is significantly impeded (e.g. excessive costs invoiced by the cloud service provider).

b. The signatory shall have the power to mandate a third party to perform its right of audit. Among others, this third party may be the ISCR where it is not the signatory.
c. When the ISCR is not the signatory, the ISCR shall have the right to access the audit data that are of relevance for it, through the signatory.

33. Performance of the right of audit:
    a. The signatory may perform this right of audit proportionately to the risks.
    b. A signatory can get sufficient assurance about the cloud service provider's fulfilment of its contractual obligations and management of risks associated to the services provided, especially regarding the quality, the continuity and the security of the outsourced services. The signatory can obtain such assurance by deeply reviewing cloud service provider's detailed audit reports or detailed third-party certification reports, provided that:
        - The signatory has open access to all the reports made available by the cloud service provider (as opposed to only receiving the information that the cloud service provider has been audited or certified);
        - The signatory ensures that the scope of the certification or audit report covers its needs:
            - the systems (i.e. processes, applications, infrastructure, data centre, etc.) which are relevant to the institution are in scope of the report;
            - the key controls as identified by the signatory in its risk assessment are in scope of the report.
        - The signatory assesses the available information and documentation continuously (i.e. ensure key controls are still covered in future versions of an audit report) and check that the certification or audit report is not obsolete.
        - The signatory is satisfied with the aptitude of the certifying or auditing party (e.g. rotation of the certifying or auditing company, qualification, expertise).
        - The certifications and audits are done against widely recognized standards[16] and contain a test of operational effectiveness of the key controls in place[17]: generic assessments that only confirm the existence of controls (without verifying their operational effectiveness) are not sufficient;
    c. The signatory and the ISCR should have the contractual right to request the expansion of scope of further certifications or audit reports to some systems

[16] E.g. ISO 27000 series
[17] E.g. SSAE 16 / ISAE 3402 type 2 report

and/or controls which are essential to them. Indeed to be a valuable and independent source of assurance, the certification or audit reports should cover the signatory's needs. The number and frequency of such requests for scope modification should be reasonable, legitimate from a risk management perspective and useful to more than one client of the cloud service provider.

d. When the diligence addressed under point (b) did not provide the required level of assurance, the right to audit can be exercised:
    - Either through a "pool audit", i.e. by pooling the signatory's resources with other outsourcing institutions having recourse to the same cloud service provider and having the same expectations (e.g. seeking the same level of assurance on the same shared cloud components). As part of its service offering, the cloud service provider could develop a cooperation model that facilitates this type of "pool audits".
    - Or through a "traditional" audit, performed on an individual basis by the signatory via its internal audit function or a third party acting on its behalf.

e. Considering that cloud computing solutions present a high level of technical complexity, the signatory should verify that the staff performing the audit - being its internal auditors or pool of auditors acting on its behalf, or the cloud service provider's appointed auditors - and, as appropriate, the staff reviewing the third-party certification or cloud service provider's audit reports, have acquired the right skills and knowledge to perform effective and relevant audit and/or assessment of cloud solutions, for instance by having successfully followed adequate training.

f. The scope of the signatory's audit engagement can be limited to those services that the signatory is using, as required by applicable legal and regulatory requirements.

g. The signatory's right to audit does not extend to other cloud service provider's client environments. When the performance of certain investigations or the use of certain audit techniques might create a risk for another client's environment, alternative ways to provide a similar level of assurance required by the institution should be agreed upon.

34. Apart from investment fund managers subject to Circular CSSF 18/698, the ISCR shall establish and complete the register referred to in point 26.a within six months as from the entry into force of this circular.

35. The investment fund managers subject to Circular CSSF 18/698 which have already outsourced on a cloud computing infrastructure before the entry into force of this circular do not have to submit a notification or authorisation request to the competent authority for this outsourcing as referred to in points 26.b and

26.c. They shall, however, establish and complete the register referred to in point 26.a within one year as from the entry into force of this circular.

36. The present circular is applicable with immediate effect.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Claude WAMPACH	Jean-Pierre FABER	Françoise KAUTHEN	Claude MARX
Director	Director	Director	Director General