Repealed by Circular CSSF 22/805

cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 17/656

as amended by Circular CSSF 21/785

Administrative and accounting organisation; IT outsourcing

Commission de Surveillance du Secteur Financier

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

Circular CSSF 17/656

as amended by Circular CSSF 21/785

Re: Administrative and accounting organisation; IT outsourcing

Luxembourg, 17 May 2017

To all electronic money institutions, payment institutions and PFS other than investment firms

Ladies and Gentlemen,

The purpose of this circular is to specify the implementation of Article 17(2) of the Law of 5 April 1993 on the financial sector, as amended (hereinafter "LFS") for professionals of the financial sector (hereinafter "PFS") and of Articles 11(2) and (4) and 24-7(2) and (4) of the Law of 10 November 2009 on payment services (hereinafter "LPS") for electronic money institutions and payment institutions, where they rely on a third party for IT services.

By doing so, it brings the obligations that apply to all electronic money institutions, payment institutions and PFS other than investment firms in line with the content of Circular CSSF 12/552 which applies to credit institutions and investment firms. Furthermore, it specifies the IT outsourcing conditions that apply specifically to support PFS and their branches abroad, if any.

This circular repeals and replaces Circular CSSF 05/178.

Chapter 1 of this circular is in line with the form and content of Sub-chapter 7.4. "Outsourcing" of Circular CSSF 12/552, applicable to credit institutions and investment firms. For easier management of any future developments, it has been decided to match the numbering of the paragraphs of this Chapter 1 with the paragraphs of Sub-chapter 7.4. of Circular CSSF 12/522; hence, the numbering starts at 181. Sub-section 2.1. and points 198, 199 and 201 of Sub-section 2.3. of Chapter 1 do not apply to PFS referred to in Articles 29-3, 29-4, 29-5 and 29-6 of the LFS and named "support PFS".

Chapter 2 specifies the conditions to be met by a support PFS and its branches abroad, if any, when using IT outsourcing other than that referred to in Circular CSSF 17/654 on cloud computing. It should be noted that support PFS allow creating a definite legal, regulated and supervised framework governing the outsourcing of financial sector activities. Article 41(5) of the LFS stipulates that the obligation to secrecy does not exist towards support PFS insofar as the information communicated to those professionals is provided in pursuance of a service agreement falling within one of the regulated activities and provided that this information is essential to the execution of the service agreement concerned.

The second Chapter is not linked to Circular CSSF 12/552; the numbering of its paragraphs is therefore disconnected from the numbering of the preceding Chapter.

Commission de Surveillance du Secteur Financier

TABLE OF CONTENTS

Chapter 1. Outsourcing

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

Whereas an IT outsourcing, or a chain of outsourcing exclusively composed of IT outsourcing, relies on a cloud computing infrastructure as defined in Circular CSSF 17/654, the provisions of this circular do not apply. In such a case, the professional of the financial sector shall comply with the requirements of Circular CSSF 17/654.

For the purposes of this circular, the term "activity" shall refer to the operational functions, activities and provisions of services referred to in the first paragraph. 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 shall be deemed to be "material".

Section 1. General outsourcing requirements

182. Outsourcing should not result in non-compliance with the rules on central administration.

The outsourcing institution shall in particular comply with the following requirements:

- The strategic functions or core functions cannot be outsourced;
- The institution shall retain the necessary expertise to effectively monitor the outsourced services or functions and manage the risks associated with the outsourcing;
- Data protection shall be guaranteed at all times;
- Outsourcing does not relieve the institution of its legal and regulatory obligations or its responsibilities to its customers. It shall not result in any delegation of the institution's responsibility to the subcontractor, except as regards the obligation of the professional secrecy where the subcontractor acts under Article 41(5) of the LFS;
- The final responsibility of the risk management associated with outsourcing is incumbent upon the authorised management of the institution which is outsourcing;
- The institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection;

- The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions;
- The institution which intends to outsource a material activity shall obtain prior authorisation from the competent authority. A notification to the competent authority stating that the conditions laid down in this circular are complied with is sufficient where the institution resorts to a Luxembourg credit institution or a support PFS. This bullet point does not apply to IT outsourcing[1];
- Any institution which intends to rely on a material IT outsourcing[2] must submit a prior notification concerning its project to the competent authority using the forms available on the CSSF website. This notification must be provided at least three (3) months before the planned outsourcing comes into effect. When resorting to a support PFS governed by Articles 29-3 to 29-6 of the LFS, this period shall be reduced to one (1) month before the planned outsourcing comes into effect. Any outsourcing for which the notification does not comply with these two (2) requirements (use of the correct form; compliance with the time limits) will be considered as non-notified;
  - In the absence of a reaction from the competent authority (additional information request, partial or total refusal of the project), the institution may implement the material IT outsourcing upon expiry of the time limit of three (3) or one (1) month(s), respectively, starting from the notification date;
  - In case of reaction by the competent authority (additional information request, partial or total refusal of the project), the competent authority may decide to suspend the time limit;
  - In any event, the supervised institutions remain fully responsible for complying with all the relevant laws and regulations as regards the planned outsourcing projects;
  - The absence of a reaction from the competent authority during the notification process is without prejudice to the supervisory measures or the application of binding measures and/or

[1] IT outsourcing means an agreement of any form between a supervised entity and a service provider (including of the same group) by which that service provider performs an IT process, an IT service or an IT activity that would otherwise be undertaken by the supervised entity itself. The processes, services or activities provided shall exclusively be IT-related.

[2] FAQs on the assessment of the materiality of an IT outsourcing are available on our website (https://www.cssf.lu/en/Document/faq-on-the-assessment-of-it-outsourcing-materiality/)

administrative sanctions which it might take at a later stage as part of the ongoing supervision, where it appears that these outsourcing projects do not comply with the applicable legal and regulatory framework;

- The access of the CSSF, the *réviseur d'entreprises agréé* (approved statutory auditor) and the internal control functions of the institution to the information relating to the outsourced activities shall be guaranteed in order to enable them to issue a well-founded opinion on the adequacy of the outsourcing. This access implies that they may also verify the relevant data kept by an external partner and, in the cases provided for in national law, have the power to perform on-site inspections of an external partner. The aforementioned opinion may, where appropriate, be based on the reports of the subcontractor's external auditor.

183. The outsourcing institution shall base its decision to outsource on a prior and in-depth 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, the expected results of the outsourcing and an in-depth evaluation of the risks of the outsourcing project as regards financial, operational, legal and reputational risks.
184. Special attention should be paid to the outsourcing of critical activities in respect of which the occurrence of a problem may have a significant impact on the institution's ability to meet the regulatory requirements or even to continue its activities.
185. Special attention should be paid to the concentration and dependence risks which may arise when large parts of activities or important functions are outsourced to a single provider during a sustained period.
186. The institutions shall take into account the risks associated with the outsourcing "chains" (where a service provider outsources part of its outsourced activities to other service providers). In this respect, they shall take particular account of the safeguarding of the integrity of the internal and external control. Moreover, the institution shall ensure to provide the CSSF with any elements proving that the sub-outsourcing process is under control.
187. The outsourcing policy should consider the impact of outsourcing on the institution's business and the risks it faces. It shall include reporting requirements to which the service providers and control mechanism which the institution implements in this respect are subject from inception to the end of the outsourcing agreement. Outsourcing may, in no circumstances, lead to the circumvention of any regulatory restrictions or prudential measures of the CSSF or challenge the CSSF's supervision.

188. Special attention should be paid to the continuity aspects and the revocable nature of outsourcing. The institution shall be able to continue its critical functions in case of exceptional events or crisis. In this respect, the outsourcing agreements shall not include termination clauses or service termination clauses because of reorganisation measures or a winding-up procedure applied to the institution, or, where applicable, bankruptcy, controlled management, suspension of payments, compositions and arrangements with creditors aimed at preventing bankruptcy or other similar proceedings.[3] The institution shall also take the necessary measures to be in a position to adequately transfer the outsourced activities to a different provider or to perform those activities itself whenever the continuity or quality of the service provision are likely to be affected.

189. For each outsourced activity, the institution shall designate from among its employees a person who will be in charge of managing the outsourcing relationship and managing access to confidential data.

Section 2. Specific IT outsourcing requirements

190. The institution shall implement an IT policy which covers all IT activities spread out among the institution and all the actors in the outsourcing chain. The IT organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the institution and the procedures manual shall be adapted accordingly. The institution's continuity plan shall be established in accordance with the continuity plan of its subcontractor(s).

191. The IT system security policy of the institution should consider the personal security established by its subcontractor(s) in order to ensure the overall consistency.

192. IT outsourcing may cover consulting, development and maintenance services (Sub-section 2.2.), hosting services (Sub-section 2.3.) or IT system management/operation services (Sub-section 2.1.).

Sub-section 2.1. IT system management/operation services

193. The institutions may contractually use services for the management/operation of their systems:
    - In Luxembourg, solely from:
        - a credit institution or a financial professional holding a support PFS authorisation in accordance with Articles 29-3 and 29-4 of the LFS (primary IT systems operators of the financial sector also called "OSIP" or secondary IT systems and communication networks operators of the financial sector also called "OSIS");

[3] *This provision differs from the equivalent provision of point 188 of Circular CSSF 12/552 as it has been adapted to the types of entities concerned.*

- an entity of the group to which the institution belongs and which exclusively deals with group transactions, provided that these systems do not include any readable confidential data on the customers. Otherwise, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection.

- Abroad, from:
  - any IT service provider, including from an entity of the group to which the institution belongs, provided that these systems do not include any readable confidential data on customers. Otherwise, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection.

Sub-section 2.2. Consulting, development and maintenance services

194. The consulting, development and maintenance services may be contracted with any IT service provider, including an IT service of the group to which the institution belongs or a support PFS.

195. By default, third-party subcontractors other than support PFS which provide consulting, development or maintenance services shall operate outside the IT production system. If an exceptional situation requires an intervention on the production system and if the access to confidential data cannot be avoided, the institution shall ensure that the third party in question is supervised throughout its mission by a person of the institution in charge of IT. Formal agreement of the institution is required for each intervention on the production system, except interventions carried out by a support PFS as part of its mandate.

196. Any change in the application functionality by a third party - other than the changes relating to corrective maintenance - shall be submitted for approval to the institution prior to its implementation.

197. The institution shall ensure that there are, if needed, no legal obstacles to obtain access to the operating systems which have been developed by this third-party subcontractor. This can be achieved, for example, when the institution is the legal owner of the programmes. The institution shall ensure that it is possible to continue operating the applications which are critical for the activity in case the subcontractor defaults, for a period compatible with a transfer of this outsourcing to another subcontractor or a taking over of the applications concerned by the institution itself.

Sub-section 2.3. Hosting services and infrastructure ownership

198. The IT infrastructure may be owned by the institution or be provided by the subcontractor.

Where the IT infrastructure includes confidential data, only the staff of the support PFS or of the Luxembourg credit institution can work either on their premises or those of the financial professional without any specific supervision by the staff of the institution, provided that the service is provided under Article 41(5) of the LFS and is the subject of a service contract enabling this autonomy. Where the subcontractor is not a support PFS or a Luxembourg credit institution, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. Otherwise, the subcontractor cannot intervene on the premises of the institution without being accompanied, throughout its mission, by a person of the institution in charge of IT.

Where the IT infrastructure does not include confidential data, express approval of the institution is required for each intervention on the IT infrastructure, except interventions carried out by a support PFS as part of its mandate.

199. It is not mandatory for the processing centre to be physically located on the premises of the entity which is contractually responsible for the management of the IT systems. Whether the processing centre is in Luxembourg or abroad, it is thus possible that the hosting of the site is entrusted with another provider than that which provides IT system management services. In this case, the institution shall ensure that the principles contained in this sub-chapter are complied with by the entity which is contractually responsible for the management of IT systems and that the sub-outsourcing process is under control.

200. Where the processing centre is in Luxembourg, it may be hosted at a provider other than a credit institution or a support PFS, provided that it has no physical and logical access to the institution's systems.

201. Where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein unless it is protected. The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions. The institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained.

Section 3. Additional general requirements

202. In order to enable the institution to assess the reliability and comprehensiveness of the data produced by the IT system as well as their compatibility with the accounting and internal control requirements, there should be one person among its employees with the required IT knowledge to understand both the impact of the programmes on the accounting system and the actions taken by the third party within the context of the provided services.

The institution shall also have, on its premises, sufficient documentation on the programmes used.

203. In case of IT service provision via telecommunication, the institution shall ensure that:
- sufficient safeguards are taken in order to avoid that non-authorised persons access its system. The institution shall, in particular, make sure that telecommunications are encrypted or protected through other available technical resources likely to ensure the security of communication;
- the IT link enables the Luxembourg institution to have quick and unfettered access to the information stored in the processing unit (i.e. through an adapted access path and debit and through data recovery).

204. The institution shall ensure that the capture, printing, backup, storage and archiving mechanisms guarantee confidentiality of data.

205. Outsourcing shall not result in the transfer of the financial and accounting function to a third party. The institution shall have, at the closing of each day, the balance of all accounts and of all accounting movements of the day. The system shall allow keeping regular accounts in accordance with the rules applicable in Luxembourg and thus respecting the form and content rules imposed by the Luxembourg accounting laws and regulations.

206. Where the institution operates abroad by using services of professional intermediaries (even if they are part of the group to which the institution belongs) or where it has branches or representative offices, any access by these intermediaries or representatives and employees of these offices and branches to its IT system in Luxembourg shall be approved by the CSSF.

Section 4. Documentation

207. Any outsourcing of activities, whether material or not, including the one carried out within the group to which the institution belongs, shall be in line with a written policy requiring approval from the authorised management and including the contingency plans and exit strategies. Any outsourcing approval shall be the subject of an official and detailed contract (including specifications).

208. The written documentation should also provide a clear description of the responsibilities of the two parties as well as the clear communication means accompanied by an obligation for the external service provider to report any significant problem having an impact on the outsourced activities as well as any emergency situation.

209. The institutions shall take the necessary measures to ensure that the internal control functions have access to any documentation relating to the outsourced activities, at any time and without difficulty, and that these functions retain the possibility to exercise their controls.

Chapter 2. Using IT outsourcing other than that referred to in Circular CSSF 17/654 on cloud computing by a support PFS and its branches abroad, if any

A. Support PFS and their branches acting as OSIP or OSIS may, for their services of system operators, rely on infrastructures belonging to their group, on the condition that the services provided by the group or their subcontractors, if any, are limited to those requiring a physical presence on these infrastructures and excluding any management of systems containing data and processing to be carried out by the support PFS. Infrastructure shall mean the IT resources that are necessary to host the systems and data under the management of the OSIP or OSIS.

In this case, the support PFS shall, in particular, ensure they have permanent control over the actions taken by the group for their account. Where this outsourcing involves the presence on the infrastructure concerned of information subject to the professional secrecy of their financial professional customers, and in particular, if the information relates to the final customers of the financial professionals, the support PFS shall be required to obtain the approval of the financial professionals concerned before outsourcing.

B. The support PFS and their branches may choose to outsource part or all of their internally used IT to a third party provider. Internally used IT means IT that excludes the one proposed as a service to third parties or the one used by the services proposed to third parties[4]. The support PFS concerned shall give prior notification of their choice to the CSSF, including when they concern their branches, by confirming how they comply with the elements of this circular. Where the outsourcing involves information subject to the professional secrecy of their financial professional customers, and in particular, information relating to the final customers of the financial professionals, the support PFS shall be required to obtain the approval of the financial professionals concerned before outsourcing.

C. Branches of support PFS may propose services relying on an infrastructure established in the host country in which they are established to their customers of the host country. This infrastructure may be outsourced to a local provider, on the condition that the services provided by this provider and its subcontractors, if any, are limited to those requiring a physical presence on these infrastructures and excluding any management of systems containing data and processing to be carried out by the support PFS or its branch. The branch shall apply the principles laid down in this circular, and the registered office in Luxembourg shall keep the appropriate control of the services provided by its branch. The branches shall obtain approval for this local outsourcing from the financial professionals concerned.

D. Except in specific cases requiring a specific authorisation from the CSSF based on duly justified arguments, the branches of support PFS may not provide system operation services to the registered office, except for internally used services. Such a situation would mean that a branch would provide system operation services to the customers of the registered office thereby emptying the support PFS of its substance.

[4] *For example, corporate email, document storage, internal accounting, VoIP telephony, CRM, etc.*

Entry into force and various provisions

This circular enters into force with immediate effect. It repeals and replaces Circular CSSF 05/178.

Yours faithfully,

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Jean-Pierre FABER Director	**Françoise KAUTHEN** Director	**Claude SIMON** Director
Simone DELCOURT Director	**Claude MARX** Director General	

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu