cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 22/806

Outsourcing arrangements

Commission de Surveillance du Secteur Financier

Circular CSSF 22/806

Re:Outsourcing arrangements

Luxembourg, 22 April 2022

To all credit institutions and professionals of the financial sector within the meaning of the Law of 5 April 1993 on the financial sector (LFS)

To all payment institutions and electronic money institutions within the meaning of the Law of 10 November 2009 on payment services (LPS)

To all investment fund managers subject to Circular CSSF 18/698

To all undertakings for collective investment in transferable securities subject to Part I (UCITS) of the UCITS Law which designate a management company within the meaning of the UCITS Law

To all central counterparties (CCPs), including Tier 2 third-country CCPs, complying with the relevant requirements of EMIR

To all approved publication arrangements (APAs) with a derogation and authorised reporting mechanisms (ARMs) with a derogation within the meaning of the LFS

To all market operators operating a trading venue within the meaning of the LFS

To all central securities depositories (CSDs)

To all administrators of critical benchmarks

Ladies and Gentlemen,

Supervised entities that fall under the scope of the Law of 5 April 1993 on the financial sector (**LFS**) and of the Law of 10 November 2009 on payment services (**LPS**) are required to adopt robust internal governance arrangements, which shall include a clear organisational structure, adequate internal control mechanisms, including sound administrative and accounting procedures and practices allowing and promoting sound and effective risk management, as well as control and security mechanisms for their IT systems.

The European Banking Authority (**EBA**) has issued revised Guidelines on outsourcing arrangements (**EBA/GL/2019/02** or the **Guidelines**). The CSSF, in its capacity as competent authority, applies the Guidelines and consequently, with a view to contribute to supervisory convergence at European level, has integrated them into its administrative practice and regulatory approach.

While the Guidelines apply to credit institutions, investment firms and payment and electronic money institutions only, the CSSF has chosen to extend the scope of application of this circular in order to promote convergence on a national level. All entities referred to under point 2 are expected to duly comply with this circular, and to take implementing measures that are proportionate to the nature, scale and complexity, including their risks, of their operations.

This circular complements the framework on internal governance arrangements by specifying guiding principles and laying down additional detailed requirements[1] that supervised entities must observe when resorting to outsourcing arrangements. Therefore, this circular shall be read together with those relevant legal provisions[2] and the circulars CSSF on central administration, internal governance and risk management[3] as applicable to supervised entities.

This circular contains in one single document the supervisory requirements on outsourcing arrangements related to information and communication technology, that were previously disseminated in individual circulars.

[1] Such precisions are provided in italics in Part I and III of the circular.
[2] Outsourcing arrangements shall at all times comply with the organisational requirements for outsourcing in accordance with articles 36-2 or 37-1(5) LFS and articles 11(4) or 24-7(4) LPS, where applicable.
[3] For example, Circular CSSF 12/552 for credit institutions and Circular CSSF 20/758 for investment firms.

Commission de Surveillance du Secteur Financier

This circular is divided in three parts: the first part sets out the requirements in relation to outsourcing arrangements and includes definitions, scope of application, general principles and applicable governance requirements; the second part is dedicated to specific requirements for ICT outsourcing arrangements relying or not on a cloud computing infrastructure and the third part provides for the entry into force of this circular.

Commission de Surveillance du Secteur Financier

TABLE OF CONTENTS

Commission de Surveillance du Secteur Financier

Part I – Outsourcing arrangements

Chapter 1. Definitions, abbreviations and acronyms

1. Unless otherwise specified, terms used and defined in the LFS, the LPS and Regulation (EU) No 575/2013 shall have the same meaning in this circular. In addition, for the purposes of this circular, the following definitions apply:

Definitions:

1) Cloud services	services provided using cloud computing, that 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. *Services are considered as cloud computing services within the meaning of this circular if the conditions defined in points 135 and 136 are fulfilled.*
a. Community cloud	cloud infrastructure available for the exclusive use by a specific community of In-Scope Entities, including several In-Scope Entities of a single group.
b. Hybrid cloud	cloud infrastructure that is composed of two or more distinct cloud infrastructures.
c. Public cloud	cloud infrastructure available for open use by the general public.
d. Private cloud	cloud infrastructure available for the exclusive use by a single In-Scope Entity.
2) Competent authority	*the CSSF or the ECB as competent authority for the supervision of entities in accordance with point 2 of this circular.*

3) Core business activities	*the activities of the In-Scope Entities which are subject to an authorisation or a registration by a competent authority.*
4) Critical or important function[4]	any function that is considered critical or important as set out in points 18 to 20.
5) Function	any processes, services or activities.
6) ICT outsourcing	*an arrangement of any form between the In-Scope Entity and a service provider by which that service provider performs an ICT process, an ICT service or an ICT activity that would otherwise be undertaken by the In-Scope Entity itself. The services are pure ICT services in nature.*
7) In-Scope Entity	*all supervised entities in accordance with point 2 of this circular.*
8) Internal control functions	*the risk control function, the compliance function and the internal audit function.*
9) Intragroup outsourcing[5]	*an outsourcing by an In-Scope Entity to a service provider who belongs to the same group.* *For In-Scope Entities that are subject to supervision on a consolidated basis in accordance with their sectoral laws and regulations or that belong to a group that is subject to such consolidated supervision it is important to note that the scope of application of the provisions on intragroup outsourcing extends beyond the sole scope of such consolidated supervision.*

[4] In the context of outsourcing arrangements, the meaning of 'critical or important function' is to be read according to MiFID Law and Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. In that regard, outsourcing arrangements comprise those that relate to 'critical functions' for the purpose of the recovery and resolution framework as defined under Article 1(64) of the BRRD Law.

[5] *For credit institutions that belong to a network of a central body or are part of an institutional protection scheme (IPS) subject to the conditions laid down in Article 113(7) CRR, an outsourcing to a member of the network or of the IPS shall be considered as an intragroup outsourcing for the purpose of this circular.*

10) Key function holders	*persons who have significant influence over the direction of the In-Scope Entity but who are neither members of the management body and are not the Chief Executive Officer (CEO).* *In line with the specific provisions of Circular CSSF 12/552 and Circular CSSF 20/758, they include the heads of internal control functions and may include the Chief Financial Officer (CFO), where they are not members of the management body, and, where identified on a risk-based approach by institutions, other key function holders.* *Other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions.*
11) Management body	an In-Scope Entity's body or bodies, which are appointed in accordance with national law, which are empowered to set the In-Scope Entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include the persons who effectively direct the business of the In-Scope Entity and the directors and persons responsible for the management of the In-Scope Entity. *In accordance with relevant circulars CSSF as applicable, the term management body encompasses the notions of authorised management, board of directors/or board of managers and/or supervisory board and executive board.*
12) Member State	*Member State of the European Union. This term includes EEA countries other than EU countries as a matter of principal.*
13) a. Outsourcing	an arrangement of any form between an In-Scope Entity and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the In-Scope Entity itself.

b. Sub-outsourcing	a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider *(the "sub-contractor").* *There may be multiple sub-outsourcing arrangements within a same outsourcing arrangement.* Sub-outsourcing *may* also be referred to as a 'chain of outsourcing', or 'chain-outsourcing'.
14) Service provider	a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement. *In this context, a group entity shall be considered as a third-party entity*.
15) Third country	*a State other than a Member State of the European Economic Area.*
Abbreviations and acronyms:	
16) AML/CFT Law	*Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended*
17) BRRD Law	*Law of 18 December 2015 on the resolution, reorganisation and winding up measures of credit institutions and certain investment firms and on deposit guarantee and investor compensation schemes, as amended*
18) BRRD institution	*a credit institution or a BRRD investment firm according to Article 59-15, point 13 LFS*
19) CRR	*Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms*
20) EBA	*the European Banking Authority*
21) ECB	*European Central Bank*
22) EEA	*European Economic Area*
23) ESMA	*the European Securities and Markets Authority*

24) GDPR	*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
25) ICT	*Information and Communication Technology*
26) LFS	*Law of 5 April 1993 on the financial sector, as amended*
27) LPS	*Law of 10 November 2009 on payment services, as amended*
28) MiFID II	*Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU*
29) MiFID Law	*Law of 30 May 2018 on markets in financial instruments, as amended*
30) UCITS Law	*Law of 17 December 2010 relating to undertakings for collective investment, as amended*

Chapter 2. Scope of application and proportionality

2. This circular defines the supervisory expectations that must be complied with when resorting to outsourcing arrangements.

This circular applies in full to the following In-Scope Entities:

- credit institutions[6] [7], including their branches, within the meaning of the LFS. Branches in Luxembourg of credit institutions incorporated in a third country shall be deemed to be included in the notion of credit institution;

[6] The ECB is the competent authority for the prudential supervision of significant credit institutions (significant institutions – SIs). SIs shall refer to the relevant ECB rules (if any).
[7] This circular shall apply to (mixed) financial holding companies that are approved in accordance with Article 34-2 LFS. See also Circular CSSF 12/552, point 3, Part I.

- investment firms, including their branches, within the meaning of the LFS. Branches in Luxembourg of investment firms incorporated in a third country shall be deemed to be included in the notion of investment firm;

*- payment institutions and electronic money institutions, including their branches, (each referred to as a **payment institution**) within the meaning of the LPS. Branches in Luxembourg of payment institutions incorporated in a third country shall be deemed to be included in the notion of payment institution. Account information service providers (**AISP**) that only provide the service in point 8 of Annex of the LPS are not included in the scope of application of this Circular. Any reference made in this Circular to 'payment services' includes payment services or issuance of electronic money provided by electronic money institutions;*

*- other professionals of the financial sector (**PFS**) including their branches, within the meaning of the LFS. Branches in Luxembourg of PFS incorporated under foreign law shall be deemed to be included in the notion of PFS;*

- POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[8]. All provisions that apply to payment institutions shall also apply to POST Luxembourg.

This Circular applies also in full to the following entities established in Luxembourg when performing ICT outsourcing:

*- investment fund managers incorporated under Luxembourg law within the meaning of Circular CSSF 18/698 (**IFMs**). For the sake of clarity, the relevant provisions related to outsourcing of Circular CSSF 18/698 do not apply to IFMs in case of ICT outsourcing arrangements;*

*- undertakings for collective investment in transferable securities subject to Part I (**UCITS**) of the UCITS Law which designate a management company within the meaning of the UCITS Law;*

*- central counterparties (**CCPs**) within the meaning of Article 2(1) of EMIR[9] , including Tier 2 third-country CCPs within the meaning of Article 25(2a) of EMIR, complying with the relevant requirements of EMIR in accordance with point (a) of Article 25(2b) of EMIR;*

*- approved publication arrangements (**APAs**) with a derogation and authorised reporting mechanisms (**ARMs**) with a derogation within the meaning of the LFS;*

- market operators operating a trading venue within the meaning of the LFS;

[8] For the sake of clarity, the wording "postal financial services" has the meaning provided for in Article 1 of the Law of 15 December 2000 as amended.
[9] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

- *central securities depositories (**CSDs**) within the meaning of point (1) of Article 2(1) of the CSDR[10]; and*
- *administrators of critical benchmarks within the meaning of point (25) of Article 3(1) of the Benchmark Regulation[11] .*

This Circular must be complied with by In-Scope Entities when designing the internal governance arrangements in the context of their business model taken as a whole, giving in particular due consideration to those activities that are regulated by the LFS, the LPS or any other national law conferring a competence to the CSSF. Consequently, this Circular also applies when In-Scope Entities provide investment services and perform investment activities in accordance with the MiFID Law, develop internal governance arrangements in the context of the AML/CFT Law or provide asset management services and depositary tasks for Undertakings for Collective Investments established in Luxembourg.

*Branches in Luxembourg of the aforementioned types of entities that are part of a legal entity whose head office is located in a different Member State of the EEA (**EEA branches**) are subject to the supervision of the competent authority of that Member State (home Member State). However, as the CSSF is competent for ensuring that EEA branches comply with the specific requirements laid down in the thematic or sectoral frameworks[12], this Circular applies if EEA branches outsource functions that belong to areas for which the CSSF retains an oversight responsibility. While this Circular does not impose specific requirements with regards to internal governance arrangements of EEA branches, such branches are nevertheless expected to adopt internal governance arrangements which are comparable to those provided for in this Circular, in coordination with their head office.*

3. The provisions of this Circular shall apply to all In-Scope Entities on *an individual* basis. Credit institutions and investment firms shall also comply with this Circular on a sub-consolidated and consolidated basis*, taking into account their prudential scope of consolidation.* Credit institutions and investment firms that are a parent undertaking shall ensure that the internal governance arrangements, processes and mechanisms in their subsidiaries are consistent,

[10] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.
[11] Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014.
[12] notably in the context of investment services in accordance with the MiFID Law, the AML/CFT Law, the provision of asset management services and depositary tasks for Undertakings for Collective Investments established in Luxembourg.

well integrated and *appropriate* for the effective application of this Circular at all relevant levels *of supervision*[13].

4. In-Scope Entities shall, when complying with this Circular, have regard to the principle of proportionality. *According to this principle, In-Scope Entities shall take implementing measures that are proportionate to their size and their internal organisation as well as to the nature, scale and complexity of their activities or services, including their risks. As such, In-Scope Entities that are large, complex or engage in risky activities or services shall adopt a more robust framework for their central administration, internal governance and risk management. By contrast, In-Scope Entities may apply a less elaborated framework where justified by their size and internal organisation as well as by the nature, scale and complexity of their activities or services, including their risks.*

5. That said, outsourcing arrangements may have an impact on the risk profile of the In-Scope Entities, notably the operational risk they may be exposed to (e.g. disruption risk). Consequently, In-Scope Entities may need to enhance their internal control framework and procedures to integrate this modified risk dimension into their entity-wide risk management framework.

6. To support the appropriate implementation of this Circular, In-Scope Entities shall document their proportionality analysis in writing and have their conclusions approved by the management body.

Chapter 3. General principles governing outsourcing arrangements and intragroup outsourcing

Sub-chapter 3.1 General principles governing outsourcing arrangements

7. Outsourcing is a means for In-Scope Entities to get relatively easy access to expertise including in the space of new technologies and to achieve economies of scale and therefore improve cost efficiency. However, the implementation of outsourcing arrangements by In-Scope Entities creates specific risks and shall be subject to specific requirements in accordance with articles 36-2 LFS, 37-1(5) LFS, 11(4) LPS and 24-7(4) LPS, where applicable.

[13] Where a waiver has been granted pursuant to Article 10 CRR to cooperative societies or Article 7 CRR, the provisions of this circular shall be applied at the level of the parent undertaking including its subsidiaries or by the central body and its affiliates as a whole.

Outsourcing arrangements shall be subject to the following principles:

- Outsourcing arrangements shall be subject to appropriate oversight and may, in no circumstances, lead to the circumvention of the spirit and letter of regulatory requirements or prudential measures.

- When outsourcing operational tasks to a service provider, the In-Scope Entity shall ensure that those operational tasks are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports in line with section 4.3.3 and with section 4.2.6 and sub-section 4.3.2.3, respectively.

- The responsibility of the management body for the In-Scope Entity and all its activities can never be outsourced:

- *Any outsourcing that would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the In-Scope Entities towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the In-scope Entity's authorisation was granted, shall not be permitted.*
- *The In-Scope Entity remains fully responsible for compliance with regulatory requirements including in the case of sub-outsourcing as sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the In-Scope Entity must determine whether sub-outsourcing is authorized and adapt its internal governance and risk management framework with regard to sub-outsourcing, in particular regarding critical or important outsourcing arrangements, while the initial service provider also has monitoring obligations.*

- Outsourcing arrangements shall not create undue operational risks. The risks to be considered include those associated with the relationship with the service provider, the risk caused by allowing for sub-outsourcing, the concentration risk posed by multiple outsourcing arrangements to the same service provider and/or the concentration risk posed by outsourcing critical or important functions to a limited number of service providers. In-Scope Entities shall in any case manage concentration and dependence risks appropriately.

- Outsourcing shall not impair the quality and independence of In-Scope Entities' internal controls or the ability of those entities to oversee and supervise compliance with regulatory requirements and to continue their activities under a going concern.

- Outsourcing must not lead to a situation where In-Scope Entities would be in breach with legal or regulatory requirements on central administration and become empty shells that lack the substance to remain authorised. To this end, management bodies shall ensure that, including in a context of an outsourcing of functions to a parent entity or other group entities, sufficient resources are

available to appropriately support and ensure the performance of their responsibilities, including overseeing the risks and managing the outsourcing arrangements.

- When outsourcing, In-Scope Entities must ensure that all requirements of this Circular are met on an ongoing basis. Functions that are considered critical under a resolution perspective may also be outsourced subject to not creating impediments to the resolvability of the BRRD institution.

8. When performing outsourcing arrangements that involve information subject to confidentiality requirements, In-Scope Entities shall put in place appropriate confidentiality arrangements and ensure compliance with article 41(2a) LFS or article 30(2a) LPS, where applicable.

9. In-Scope Entities shall comply with GDPR and the requirements of the Luxembourg competent authority in this area, namely the "Commission Nationale pour la Protection des Données" (CNPD).

10. Outsourcing may, in no circumstances, hamper the performance of supervisory powers by competent authorities with regard to all aspects of supervisory relevance. Outsourcing arrangements shall in particular not impact the competent authorities' ability to oversee and supervise In-Scope Entities' compliance with legal or regulatory requirements under a going concern or BRRD institutions' regulatory compliance from a resolution perspective.

Sub-chapter 3.2 Intragroup outsourcing

11. *Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group. Intragroup outsourcing is therefore subject to the same regulatory framework and conditions as outsourcing to service providers outside the group. Where In-Scope Entities intend to outsource to entities within the same group, they shall also ensure that the reason for selecting a group entity is based on objective reasons. In particular, the group entity shall be suitable and the outsourcing arrangement may not expose the In-Scope Entities to an undue conflict of interest.*

12. *When outsourcing within the same group, In-Scope Entities may have a higher level of control over and information about the outsourced function and the service provider, which they could take into account in their risk assessment. In-Scope Entities shall however not exclusively rely on their group entities for the management of the outsourcing and shall design procedures for the performance of appropriate monitoring and oversight at the level of the In-Scope Entity itself to ensure compliance with the requirements set out in this Circular*.

13. *Subject to the general principles set out in sub-chapter 3.1*, In-Scope Entities that use centrally provided governance arrangements shall *therefore* comply with the following:

a. where In-Scope Entities have outsourcing arrangements with service providers within the group, the management body of the In-Scope Entity retains, also for these outsourcing arrangements, full responsibility for compliance with the regulatory requirements and the effective application of this Circular;

b. *where In-Scope Entities have outsourcing arrangements with a service provider within the group, the In-Scope Entity shall ensure that those outsourcing arrangements, including operational tasks that are outsourced, are effectively performed. In-Scope Entities shall perform an appropriate monitoring and auditing of outsourcing arrangements, including through the receiving of appropriate reports, in line with section 4.3.3. and with section 4.2.6 and sub-section 4.3.2.3, respectively.*

14. In addition to point 13 above, In-Scope Entities within a group shall take into account the following:

a. where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), In-Scope Entities shall ensure that both the independent monitoring of the service provider and its appropriate oversight by each In-Scope Entity is possible, including by receiving, at least annually and upon request, from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring *and by challenging those reports*. In addition, In-Scope Entities shall receive from the centralised monitoring function a summary of the relevant *outsourcing* audit reports and, upon request, the full audit report.

   The management body of In-Scope Entities shall determine whether the extent and the contents of these reports are consistent and appropriate and shall take action if these reports do not enable it to comply with the requirements on internal governance and on risk management as laid down in other relevant circulars CSSF;

b. In-Scope Entities shall ensure that their management body shall be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, *comprising* legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes *and accept them or take action as appropriate*;

c. where In-Scope Entities within the group rely on a central pre-outsourcing assessment of outsourcing arrangements, each In-Scope Entity shall receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process *and accept it or take action as appropriate*;

d. for In-Scope Entities within a group, the register *as referred to in section 4.2.7* may be kept centrally. Where the register of all existing outsourcing arrangements, is established and maintained centrally within a group, the competent authorities and all In-Scope Entities shall be able to obtain the individual register without undue delay. This register shall include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group. *In-Scope Entities shall be satisfied that the register complies with the provisions set out in Section 4.2.7 on Documentation requirements;*

e. *in relation to their exit strategies,* where In-Scope Entities rely on an exit plan for a critical or important function that has been established at group level, all In-Scope Entities shall receive a summary of the plan and be satisfied that the plan can be effectively executed *in accordance with the provisions set out in Section 4.3.4 on Exit plans*;

f. In-Scope Entities within a group may rely on centrally established business continuity plans regarding their outsourced functions. In-Scope Entities shall receive a summary of the plan *and be satisfied that the plan complies with the provisions of Section 4.2.5 on Business continuity plans*.

Chapter 4. Governance of outsourcing arrangements

Sub-chapter 4.1 Assessment of outsourcing arrangements

Section 4.1.1 Outsourcing

15. In-Scope Entities shall establish whether an arrangement with a third party falls under the definition of outsourcing. Within this assessment, consideration shall be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by In-Scope Entities, even if the In-Scope Entity has not performed this function in the past itself.

16. Where an arrangement with a service provider covers multiple functions, In-Scope Entities shall consider all aspects of the arrangement within their assessment, e.g. if the service provided includes the provision of data storage hardware and the backup of data, both aspects shall be considered together.

17. As a general principle, In-Scope Entities shall not consider the following as outsourcing:

a. a function that is legally required to be performed by a service provider, e.g. statutory audit;

b. market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);
c. global network infrastructures (e.g. Visa, MasterCard);
d. clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;
e. global financial messaging infrastructures that are subject to oversight by relevant authorities;
f. correspondent banking services; and
g. the acquisition of services that would otherwise not be undertaken by the In-Scope Entity (e.g. advice from an architect, legal *advice* and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the In-Scope Entity's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards[14], card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).

Section 4.1.2 Critical or important functions

18. In-Scope Entities shall always consider a function as critical or important in the following situations:

a. where a defect or failure in its performance would materially impair:
   i. their continuing compliance with the conditions of their authorisation and/or their other *legal* and regulatory obligations*;*
   ii. their financial performance; or
   iii. the soundness or continuity of their services and activities;
b. when operational tasks of internal control functions *or operational tasks of the financial and accounting function as referred in points 21 to 29* are outsourced;
c. when *credit institutions and payment institutions* intend to outsource functions of banking activities or payment services to an extent that would require authorisation[15] by *the relevant* competent authority *as referred to in points 61 to 63*.

19. In the case of *BRRD* institutions, particular attention shall be given to the assessment of the criticality or importance of functions if the outsourcing

[14] This does not cover the issuance of payment instruments such as the issuance of credit cards, which is a regulated payment service under the LPS.
[15] See the activities listed in *Annex I of LFS and in Annex of LPS related to payment services.*

concerns functions related to core business lines and critical functions *according to the BRRD Law*[16] and identified by these institutions using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778[17]. Functions that are necessary to perform activities of core business lines or critical functions shall be considered as critical or important functions for the purpose of this Circular, unless the *BRRD* institution's assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the operational continuity of the core business line or critical function.

20. When assessing whether an outsourcing arrangement relates to a function that is critical or important, In-Scope Entities shall take into account, together with the outcome of the risk assessment outlined in *points 66 to 70* at least the following factors:

a. whether the outsourcing arrangement is directly connected to *core business activities*;

b. the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:

i. short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;

ii. business continuity and operational resilience;

iii. operational risk, including conduct, ICT and legal risks;

iv. reputational risks;

v. where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;

c. the potential impact of the outsourcing arrangement on their ability to:

i. identify, monitor and manage all risks;

ii. comply with legal and regulatory requirements;

[16] *Critical functions according to Article 1(64) of BRRD Law means activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of a BRRD institution or group, with particular regard to the substitutability of those activities, services or operations.*

[17] Commission Delegated Regulation (EU) 2016/778 of 2 February 2016 supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary ex post contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines.

iii. conduct appropriate audits regarding the outsourced function;

d. the potential impact on the services provided to its clients;

e. all outsourcing arrangements, the In-Scope Entity's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;

f. the size and complexity of any business area affected;

g. the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;

h. the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');

i. the ability to reintegrate the outsourced function into the In-Scope Entity, if necessary or desirable;

j. the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the In-Scope Entity and its clients, including but not limited to compliance with *GDPR*.

Section 4.1.3 Outsourcing arrangements relating to internal control functions

21. Outsourcing arrangements of internal control functions shall not effectively result in the transfer of these functions as a whole to the service provider(s). Therefore, outsourcing arrangements shall be limited, in principle, to operational tasks of these functions.

22. Outsourcing arrangements of operational tasks of the internal control functions shall not undermine the permanence of the internal control arrangements and functions of the In-Scope Entity or their continued effectiveness. In practice this means that outsourcing arrangements shall be proportionate and shall not result in the effective carving out of the substance of the In-Scope Entities' internal control functions.

23. In accordance with the requirements of section 4.3.1.2, In-Scope Entities shall ascertain that the service provider complies with applicable suitability requirements and has appropriate and sufficient technical knowledge and experience. In particular, the service provider shall demonstrate an appropriate and up-to-date knowledge of the regulatory framework that applies to the In-Scope Entity.

24. When outsourcing operational tasks of the internal control functions, the service provider shall be placed under the oversight of and report to the person in charge of the relevant internal control function of the In-scope Entity (e.g. the Chief Compliance Officer, the Chief Risk Officer or the Chief Internal

Auditor). Where In-scope Entities outsource the full range of operational tasks of their internal control function, the service provider shall report to the member of the management body in charge of the internal control function.

25. In the context of the internal audit function, the service provider shall also have a direct access to the management body in its supervisory functions or, where appropriate, to the chairperson of the audit committee. In addition, the service provider shall carry out the internal audit operational tasks in accordance with the In-Scope Entity's internal audit plan and work programme, document the work and the findings of each mission in sufficient detail and issue a dedicated report on each mission. All documents shall be drafted in French, German or English and delivered to the person in charge of the internal audit function, to the management body and, where applicable, to the audit committee.

Section 4.1.4 Outsourcing arrangements relating to the financial and accounting function

26. Outsourcing arrangements of the financial and accounting function shall not effectively result in the transfer of this function as a whole to the service provider(s). Therefore, outsourcing arrangements shall be limited, in principle, to operational tasks of this function. Outsourcing arrangements of operational tasks of the financial and accounting functions shall not undermine the permanence of the central administration of the In-Scope Entity.

27. *When outsourcing operational tasks of the accounting function, In-Scope Entities shall have, at the closing of each day, unconditional and unrestricted access to the balance of all accounts and of all accounting movements of the day in order to provide the competent authority or any other body, as required by applicable laws and regulations, with this information.*

28. When using an accounting system that is located outside of Luxembourg (accounting system hosting outsourcing) independently or in connection with the outsourcing of operational tasks of the accounting function, the In-Scope Entity shall have, at the end of each day, a secure backup of all end of day accounting positions, including client positions, in a readable format, to guarantee an autonomous preparation of a balance sheet, a profit and loss statement and client positions.

This backup shall be stored at the premises of the In-Scope Entity in the EEA, of a group entity located in the EEA, or of another service provider (i.e. a service provider different from the one to whom the accounting system is outsourced) located in the EEA. The accounting system shall allow keeping regular accounts in accordance with the applicable accounting framework in Luxembourg, the preparation of statutory accounts and the preparation of the prudential reports to the competent authority.

29. In case of outsourcing of the production of prudential reports, the person in charge of the financial and accounting function in the In-Scope Entity shall ensure that these reports represent faithfully the In-Scope Entity's prudential situation and are prepared in accordance with the applicable instructions. In addition, this person shall be able to ensure that the In-Scope Entity's annual accounts are prepared in accordance with the applicable accounting laws and regulations[18]*.*

Sub-Chapter 4.2 Governance framework

Section 4.2.1 Sound governance arrangements and third-party risk

30. As part of the overall internal control framework, including internal control mechanisms,[19] In-Scope Entities shall have a holistic entity-wide risk management framework extending across all business lines and internal units. Under that framework, In-Scope Entities shall identify and manage all their risks, including risks caused by arrangements with third parties. The risk management framework shall also enable In-Scope Entities to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including with regard to cyber risks.[20]

31. In-Scope Entities, taking into account the principle of proportionality, shall identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, regardless of whether or not those arrangements are outsourcing arrangements. The risks, in particular the operational risks, of all arrangements with third parties, shall be assessed in line with points 66 to 70.

32. In-Scope Entities shall ensure that they comply with all requirements under *GDPR*, including for their third-party and outsourcing arrangements.

Section 4.2.2 Sound governance arrangements for outsourcing

33. The outsourcing of functions shall not result in the delegation of the management body's responsibilities. The *management body* remains fully responsible and accountable for complying with all of their regulatory obligations *or their responsibilities to their customers*, including the ability to oversee the outsourcing of critical or important functions.

[18] The Law of 17 June 1992 relating to the annual and consolidated accounts of credit institutions governed by the laws of Luxembourg for credit institutions or the Law of 19 December 2002 as amended relating to the trade register the accounting rules and the annual accounts of companies for other In-Scope Entities.
[19] Please also refer to Articles 6, 7, 24-2 and 24-3 LPS, when applicable.
[20] Please refer to Circular CSSF 20/750 on ICT and security risk management.

34. The management body is at all times fully responsible and accountable for at least:

a. ensuring that the In-Scope Entity meets on an ongoing basis the conditions with which it must comply to remain authorised, including any conditions imposed by the competent authority;

b. the internal organisation of the In-Scope Entity;

c. the identification, assessment and management of conflicts of interest;

d. the setting of the In-Scope Entity's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);

e. overseeing the day-to-day management of the In-Scope Entity, including the management of all risks associated with outsourcing; and

f. the oversight role of the management body in its supervisory function, including overseeing and monitoring management decision-making.

35. Outsourcing shall not lower the suitability requirements applied to the In-Scope Entity's management body and key function holders. In-Scope Entities shall have adequate competence, sufficient and appropriately skilled resources to ensure an appropriate management and oversight of outsourcing arrangements.

36. In-Scope Entities shall:

a. clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;

b. allocate sufficient *skilled* resources to ensure compliance with *the* legal and regulatory requirements, including *this Circular* and the documentation and monitoring all outsourcing arrangements;

c. *for each outsourced activity, designate from among its employees a person who will be in charge of managing the outsourcing relationship(s) and managing access to confidential data; and*

d. establish an outsourcing function or designate a *sufficiently* senior staff member who is directly accountable to the management body (e.g. a key function holder of a control function) and responsible for managing and overseeing the risks of outsourcing arrangements as part of the In-Scope Entity's internal control framework and overseeing the documentation of outsourcing arrangements. *Small entities*[21] shall at least ensure a clear *and sound* division of tasks and responsibilities for the management and control

[21] *Credit institutions and investment firms shall refer to Circulars CSSF 12/552 and 20/758 to perform the assessment of small entities.*

of outsourcing arrangements and may assign the outsourcing function to a member of the In-Scope Entity's management body.

37. In-Scope Entities shall maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities'. To this end, they shall:

a. meet all the conditions of their authorisation at all times, including the management body effectively carrying out its responsibilities as set out in point 34;

b. retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;

c. exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of critical or important functions, *in particular where* operational tasks of internal control functions, *of the financial and accounting function or of core business activities* are outsourced; and

d. have sufficient *skilled* resources and capacities to ensure compliance with points a. to c. above.

38. When *setting up an* outsourcing *arrangement*, In-Scope Entities shall at least ensure that:

a. they can take and implement decisions related to their business activities and critical or important functions, including with regard to those that have been outsourced;

b. they maintain the orderliness of the conduct of their business and*, for credit institutions and payment institutions,* the banking and payment services they provide;

c. the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech);

d. appropriate confidentiality arrangements are in place regarding data and other information;

e. an appropriate flow of relevant information with service providers is maintained;

f. with regard to the outsourcing of critical or important functions, they are able to undertake at least one of the following actions, within an appropriate time frame:

i. transfer the function to alternative service providers;

ii. reintegrate the function; or

iii. discontinue the business activities that are depending on the function.

g. where personal data are processed by service providers located in the *EEA* and/or third countries, appropriate measures are implemented and data are processed in accordance with *GDPR*;

h. appropriate confidentiality arrangements are in place and ensure compliance with article 41(2a) LFS or article 30(2a) LPS, where applicable.

Section 4.2.3 Outsourcing policy

39. The management body of an In-Scope Entity that has outsourcing arrangements in place or plans on entering into such arrangements shall approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. For credit institutions and investment firms, the outsourcing policy shall, in particular, take into account the requirements *pertaining to "New Product Approval Process"*[22].

40. The policy shall include the main phases of the life cycle of outsourcing arrangements and define the principles, responsibilities and processes in relation to outsourcing. In particular, the policy shall cover at least:

a. the responsibilities of the management body in line with points 33 and 34, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;

b. the involvement of business lines, internal control functions and other individuals in respect of outsourcing arrangements;

c. the planning of outsourcing arrangements, including:

i. the definition of business requirements regarding outsourcing arrangements;

ii. the criteria, including those referred to in points 18 to 20, and processes for identifying critical or important functions;

iii. risk identification, assessment and management in accordance with points 66 to 70;

iv. due diligence checks on prospective service providers, including the measures required under points 71 to 75;

v. procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with points 43 to 46;

[22] *Please refer to Part II, sub-chapter 7.3 of Circular CSSF 12/552 for credit institutions or to Part II, sub-chapter 7.3 of Circular CSSF 20/758 for investment firms.*

vi. business continuity planning in accordance with points 47 to 50;

vii. the approval process of new outsourcing arrangements. *This process must consider the additional time requirement due to the prior notification to the competent authority in accordance with points 59 and 60*;

d. the implementation, monitoring and management of outsourcing arrangements, including:

i. the ongoing assessment of the service provider's performance in line with points 104 to 110;

ii. the procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structures, sub-outsourcing);

iii. the independent review and audit of compliance with legal and regulatory requirements and policies;

iv. the renewal processes;

e. the documentation and record-keeping, taking into account the requirements set out in points 53 to 58;

f. the exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible, taking into account possible service interruptions or the unexpected termination of an outsourcing agreement*, in line with points 111 to 113*.

41. The outsourcing policy shall differentiate between the following:

a. outsourcing of critical or important functions and other outsourcing arrangements;

b. outsourcing to service providers that are authorised by a *relevant* competent authority *in a Member State or in a third country* and those that are not;

c. intragroup outsourcing arrangements and outsourcing to entities outside the group; and

d. outsourcing to service providers located within a Member State and third countries.

42. In-Scope Entities shall ensure that the *outsourcing* policy covers the identification of the following potential effects of critical or important outsourcing arrangements and that these are taken into account in the decision-making process:

a. the In-Scope Entity's risk profile;

b. the ability to oversee the service provider and to manage the risks;

c. the business continuity measures; and

d. the performance of their business activities.

Section 4.2.4 Conflicts of interests[23]

43. In-Scope Entities shall identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.

44. Where outsourcing creates material conflicts of interest, including between entities within the same group, In-Scope Entities need to take appropriate measures to manage those conflicts of interest.

45. When functions are provided by a service provider that is part of a group or that is owned by the In-Scope Entity or its group, the conditions, including financial conditions, for the outsourced service shall be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several In-Scope Entities within a group may be factored in, as long as the service provider remains viable on a stand-alone basis; within a group this shall be irrespective of the failure of any other group entity.

46. The In-Scope Entity shall, in particular, ensure that the service provider is independent from the statutory auditor (réviseur d'entreprises agréé or cabinet de révision agréé) in charge of the statutory audit of the In-Scope Entity and from the group to which the statutory auditor belongs.

Section 4.2.5 Business continuity plans

47. *Special attention shall be paid to the continuity aspects and the revocable nature of an outsourcing arrangement. The In-Scope Entity shall be able to continue its critical functions in case of exceptional events or crisis.*

48. In-Scope Entities shall have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions.

49. Business continuity plans shall take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans shall also take into account the potential impact of the insolvency or other failures of service

[23] *Please also refer to Circular CSSF 12/552, Part II, sub-chapter 7.2 (points 165 to 174) for credit institutions or Circular CSSF 20/758, Part II, sub-chapter 7.2 (points 167 to 176) for investment firms.*

providers and, where relevant, political risks in the service provider's jurisdiction.

50. *Where the outsourcing arrangement comprises ICT systems and data of In-Scope Entities, the measures for redundancy and backup of these systems and data shall either be specified in the outsourcing agreement with the service provider or configured by the In-Scope Entities*[24]*, in line with the business continuity plan of the In-Scope Entities.*

Section 4.2.6 Internal audit function

51. The internal audit function's activities shall cover, following a risk-based approach, the review of outsourced activities. The audit plan and programme shall include, in particular, the outsourcing arrangements of critical or important functions.

52. With regard to the outsourcing process, the internal audit function shall at least ascertain:

a. that the In-Scope Entity's framework for outsourcing, including the outsourcing policy, is effectively implemented and is in line with the applicable laws and regulations, the risk strategy and the decisions of the management body;

b. the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;

c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the In-Scope Entity's risk strategy;

d. the appropriate involvement of governance bodies; and

e. the appropriate monitoring and management of outsourcing arrangements.

Section 4.2.7 Documentation requirements

53. In-Scope Entities shall maintain an updated register of information on all outsourcing arrangements at *individual level* and, as applicable, at sub-consolidated and consolidated levels, as set out in point 3, and shall appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. In-Scope Entities shall maintain the documentation of ended

[24] *In case of outsourcing to a cloud computing infrastructure, the parametrisation of continuity measures may be performed by the In-Scope Entities.*

outsourcing arrangements within the register and the supporting documentation for an appropriate period *in accordance with Luxembourg law*.

54. *For the purposes of prudential supervision,* the register shall include at least the following information for all existing outsourcing arrangements:

a. a reference number for each outsourcing arrangement;

b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the In-Scope Entity;

c. a brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider;

d. a category assigned by the In-Scope Entity that reflects the nature of the function as described under point (c) (e.g. *ICT*, *internal* control functions), which shall facilitate the identification of different types of arrangements;

e. the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any);

f. the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;

g. whether or not (yes/no) the outsourced function is considered critical or important, including a brief summary of the reasons why the outsourced function is considered *or not as* critical or important;

h. in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

i. the date of the most recent assessment of the criticality or importance of the outsourced function.

55. For the outsourcing of critical or important functions, the register shall include the following additional information:

a. the In-Scope Entities and other firms within the scope of the prudential consolidation, as applicable, that make use of the outsourcing;

b. whether or not the service provider or *sub-contractor* is part of the group or is owned by In-Scope Entities within the group;

c. the date of the most recent risk assessment and a brief summary of the main results;

d. the individual or decision-making body (e.g. the management body) in the In-Scope Entity that approved the outsourcing arrangement;

e. the governing law of the outsourcing agreement;

f. the dates of the most recent and next scheduled audits, where applicable;

g. where applicable, the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;

h. an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the In-Scope Entity or the impact of discontinuing the critical or important function;

i. identification of alternative service providers in line with point (h);

j. whether the outsourced critical or important function supports business operations that are time-critical;

k. the estimated annual budget cost;

l. the date of the prior notification to the competent authority in accordance with points 59 and 60, as applicable.

56. In-Scope Entities shall, upon request, make available to the competent authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point 54(d) (e.g. all *ICT* outsourcing arrangements*).*

57. In-Scope Entities shall appropriately document the assessments made under points 66 to 103 and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).

58. In-Scope Entities shall, upon request, make available to the competent authority all information necessary to enable the competent authority to execute *its* effective supervision, including a copy of the outsourcing agreement.

Section 4.2.8 Supervisory conditions for outsourcing

59. An In-Scope Entity that intends to outsource a critical or important function[25] shall notify in advance its plans to the competent authority using the instructions and, where available, the forms on the CSSF website. Such a notification is to be submitted at least three (3) months before the planned outsourcing comes into effect. When resorting to a Luxembourg support PFS governed by Articles 29-1 to 29-6 LFS, this notice period is reduced to one (1) month. Any planned outsourcing arrangement which has not been notified within the above notification period and/or without using the instructions and, where applicable, the forms available on the CSSF website will be considered as not notified.

60. The notification is without prejudice to the supervisory measures or the application of binding measures and/or administrative sanctions which the competent authority might take as part of its ongoing supervision, where it appears that these outsourcing projects do not comply with the applicable legal and regulatory framework.

In any event, In-Scope Entities remain fully responsible to comply with all the relevant laws and regulations as regards the planned outsourcing projects.

61. *Should credit institutions* or payment institutions *outsource* functions of banking activities or payment services to a service provider located in Luxembourg or another Member State*,* to an extent that the performance of that function *would* require authorisation or registration *where such activities would be carried out in Luxembourg*, *such an outsourcing shall take* place only if one of the following conditions is met:

a. the service provider is authorised or registered by a *relevant* competent authority *in that Member State* to perform such banking activities or payment services; or

b. the service provider is otherwise allowed to carry out those banking activities or payment services in accordance with the relevant national legal framework.

[25] An In-Scope Entity shall also notify the competent authority in case of material changes to existing outsourcing arrangements (e.g. in case such material changes impact a critical or important outsourced function or lead to an outsourcing arrangement becoming critical or important) without undue delay.

62. *Should credit institutions* or payment institutions *outsource* functions of banking activities or payment services to a service provider located in a third country, to an extent that the performance of that function *would* require authorisation or registration *where such activities would be carried out in Luxembourg*, *such an outsourcing shall take* place only if the following conditions are met:

a. the service provider is authorised or registered to provide that banking activity or payment service in the third country and is supervised by a relevant competent authority in that third country (referred to as a 'supervisory authority'); and

b. there is an appropriate cooperation agreement[26], e.g. in the form of a memorandum of understanding or college agreement, between the competent authority and the supervisory authorities responsible for the supervision of the service provider. *In-Scope Entities shall contact the CSSF in the early planning stages of their planned outsourcing arrangement to ascertain that cooperation arrangements between the CSSF and the third country supervisory authority are or can be put in place.*

63. For the purposes of points 61 and 62, the outsourcing of functions of banking activities to an extent that the performance of that function would require authorisation or registration where such activities would be carried out in Luxembourg shall apply in the event where a credit institution[27] intends to proceed to the outsourcing of a material proportion of the activity that consists in the taking of deposits and other repayable funds from the public[28].

64. *The outsourcing to a service provider located in Luxembourg that relates to services subject to an authorisation requirement in accordance with Articles 29-1 to 29-6 LFS shall take place only if one of the following conditions is met:*

a. the service provider is authorised by the CSSF in accordance with Articles 29-1 to 29-6 LFS to provide such services; or

b. the service provider is otherwise allowed to carry out those services, i.e. it is a credit institution or it is an entity falling under the scope of article 1-1(2)(c) LFS that is part of the group to which the In-Scope Entity belongs and which exclusively deals with group transactions.

[26] Cooperation agreements may take the form of a Memorandum of Understanding or of a dedicated agreement concluded between the competent authority and a third country supervisory authority in the context of the prudential supervision of a specific In-Scope Entity. A list of MoUs that have been signed by the CSSF is available on the CSSF website. The list of MoUs signed by the ECB is available on the ECB website.
[27] or POST Luxembourg.
[28] In accordance with article 2(3) LSF, persons or undertakings other than credit institutions are prohibited from carrying out the business of taking deposits or other repayable funds from the public.

Sub-chapter 4.3 Outsourcing process

Section 4.3.1 Pre-outsourcing analysis

65. Before entering into any outsourcing arrangement, In-Scope Entities shall:

a. assess if the outsourcing arrangement concerns a critical or important function;

b. assess if the supervisory conditions for outsourcing are met;

c. identify and assess all of the relevant risks of the outsourcing arrangement;

d. undertake appropriate due diligence on the prospective service provider; and

e. identify and assess conflicts of interest that the outsourcing may cause.

Sub-section 4.3.1.1 Risk assessment of outsourcing arrangements

66. In-Scope Entities shall assess the potential impact of outsourcing arrangements on their operational *capacity and* risk, shall take into account the assessment results when deciding if the function shall be outsourced to a service provider and shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.

67. The assessment shall include, where appropriate, scenarios of possible risk events, including high-severity operational risk events*, in particular when the outsourcing arrangement relates to a critical or important function of the In-Scope Entity.* Within the scenario analysis, In-Scope Entities shall assess the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events. In-Scope Entities shall document the analysis performed and their results and shall estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk. *Small entities* may use qualitative risk assessment approaches, while *other* In-Scope Entities shall have a more sophisticated approach, including, where available, the use of internal and external loss data to inform the scenario analysis.

68. When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, In-Scope Entities shall, at least:

a. identify and classify the relevant functions and related data and systems as regards their *risk* sensitivity and required security measures;

b. conduct a thorough risk-based analysis of the functions and related data and systems that are being considered for outsourcing or have been outsourced *in order to* address the potential risks, in particular the operational risks, including legal, ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced

services are or may be provided and where the data are or are likely to be stored;

c. consider the consequences of where the service provider is located (within or outside the *EEA*) *in accordance with points 61 to 64 and whether the service provider is supervised by a relevant competent authority*;

d. consider the political stability and security situation of the jurisdictions in question, including:

   i. the laws in force, including laws on data protection;

   ii. the law enforcement provisions in place; and

   iii. the insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgent recovery of the In-Scope Entity's data in particular;

e. define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the *(*intended*)* outsourcing. In-Scope Entities shall also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;

f. consider whether the service provider is a subsidiary or parent undertaking of the In-Scope Entity or is included in the scope of accounting consolidation and, if so, the extent to which the In-Scope Entity controls it or has the ability to influence its actions.

69. Within the risk assessment, In-Scope Entities shall also take into account the expected benefits and costs of the proposed outsourcing arrangement, including weighing any risks that may be reduced or better managed against any risks that may arise as a result of the proposed outsourcing arrangement, taking into account at least:

a. concentration risks, including from:

   i. outsourcing to a dominant service provider that is not easily substitutable; and

   ii. multiple outsourcing arrangements with the same service provider or closely connected service providers;

b. the aggregated risks resulting from outsourcing several functions across the In-Scope Entity and, in the case of groups of In-Scope Entities, the aggregated risks on a consolidated basis;

c. in the case of significant In-Scope Entities[29], the step-in risk, i.e. the risk that may result from the need to provide financial support to a service provider in distress or to take over its business operations; and

d. the measures implemented by the In-Scope Entity and by the service provider to manage and mitigate the risks.

70. Where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions, *or material parts thereof,* to other service providers, In-Scope Entities shall take into account:

a. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;

b. the risk that long and complex chains of sub-outsourcing reduce their ability to oversee the outsourced critical or important function and the ability of competent authorities to effectively supervise them.

Sub-section 4.3.1.2 Due diligence

71. Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, In-Scope Entities shall ensure in their selection and assessment process that the service provider is suitable.

72. In-Scope Entities shall ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, ICT, financial), the organisational structure and, if applicable, the required regulatory authorisation(s) or registration(s) to perform the function in a reliable and professional manner to meet its obligations over the duration of the draft contract.

73. Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:

a. its business model, nature, scale, complexity, financial situation, ownership and group structure;

b. the long-term relationships with service providers that have already been assessed and perform services for the In-Scope Entity;

c. whether the service provider is a parent undertaking or subsidiary of the In-Scope Entity or is part of the scope of accounting consolidation of the In-Scope Entity;

[29] *In particular entities that are in scope of art. 59-3 LFS.*

d. whether or not the service provider is supervised by *relevant* competent authorities.

74. Where outsourcing involves the processing of personal or confidential data, In-Scope Entities shall be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.

75. In-Scope Entities shall take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, with regard to service providers located in third countries and, if applicable, their sub-contractors, In-Scope Entities shall be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

Section 4.3.2 Contractual phase

76. The rights and obligations of the In-Scope Entity and the service provider shall be clearly allocated and set out in a written *outsourcing* agreement.

77. *The outsourcing agreement shall set out:*

a. a clear description of the outsourced function to be provided;

b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the In-Scope Entity;

c. the governing law of the agreement;

d. the parties' financial obligations;

e. whether the sub-outsourcing*, in particular,* of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in points 78 to 82 that the sub-outsourcing is subject to;

f. the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the In-Scope Entity if the service provider proposes to change the location(s);

g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in points 83 to 87;

h. the right of the In-Scope Entity to monitor the service provider's performance on an ongoing basis;

i. the agreed service levels, which shall include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;

j. the reporting obligations of the service provider to the In-Scope Entity, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements *(including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation)* and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;

k. whether the service provider shall take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

l. the requirements to implement and test business contingency plans;

m. provisions that ensure that the data that are owned by the In-Scope Entity can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;

n. the obligation of the service provider to cooperate with the competent authorities and*, where applicable,* resolution authorities of the In-Scope Entity, including other persons appointed by them;

o. for *BRRD* institutions, a clear reference to the national resolution authority's[30] powers, especially to Articles 59-47 LFS, 66 and 69 of the BRRD Law, and in particular a description of the 'substantive obligations' of the contract in the sense of the Articles 59-47 LFS and 66 of the BRRD Law;

p. the unrestricted right of In-Scope Entities and competent authorities to inspect and audit the service provider*, including in case of sub-outsourcing,* with regard to*, at least,* the critical or important outsourced function, as specified in points 88 to 100;

q. termination rights as specified in points 101 to 103.

Sub-section 4.3.2.1 Sub-outsourcing

78. The outsourcing agreement shall specify whether or not sub-outsourcing*, in particular* of critical or important functions, or material parts thereof, is permitted.

79. If sub-outsourcing of critical or important functions is permitted, In-Scope Entities shall determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.

[30] *means an authority as defined in point (8) of Article 1 of the BRRD Law.*

80. If sub-outsourcing of critical or important functions, *or material parts thereof,* is permitted, the written *outsourcing* agreement shall:

a. specify any types of activities that are excluded from sub-outsourcing;

b. specify the conditions to be complied with in the case of sub-outsourcing;

c. specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the In-Scope Entity are continuously met;

d. require the service provider to obtain prior specific or general written authorisation from the In-Scope Entity before sub-outsourcing data;[31]

e. include an obligation of the service provider to inform the In-Scope Entity of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set shall allow the In-Scope Entity at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;

f. ensure, where appropriate, that the In-Scope Entity has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;

g. ensure that the In-Scope Entity has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the In-Scope Entity or where the service provider sub-outsources without notifying the In-Scope Entity.

81. In-Scope Entities shall agree to sub-outsourcing *critical or important functions*, *or material parts thereof,* only if the sub-contractor undertakes to:

a. comply with applicable laws, regulatory requirements and contractual obligations; and

b. grant the In-Scope Entity and competent authority the same contractual rights of access and audit as those granted by the service provider.

82. In-Scope Entities shall ensure that the service provider appropriately oversees the *sub-contractors*, in line with the policy defined by the In-Scope Entity. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to

[31] *Please refer to* Article 28 GDPR.

a material increase of risk, including where the conditions in point 81 above would not be met, the In-Scope Entity shall exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

Sub-section 4.3.2.2 Security of data and systems

83. *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 shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.*

84. In-Scope Entities shall ensure that service providers, where relevant, comply with appropriate *ICT* security standards.

85. Where relevant (e.g. in the context of cloud or other ICT outsourcing), In-Scope Entities shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis. *Where, in the outsourcing agreement, security measures are made available by the service provider to the In-Scope Entities for personalized selection and configuration (notably for cloud outsourcing), In-Scope Entities shall ensure that proper selection and configuration take place, in line with the In-Scope Entity's security policy and requirements.*

86. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, In-Scope Entities shall adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) *which shall in particular take into account point 101 c, d and e* and information security considerations *and comply with the provisions of points 133 to 143.*

87. Without prejudice to the requirements under *GDPR*, In-Scope Entities, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. In-Scope Entities shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the In-Scope Entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).

Sub-section 4.3.2.3 Access, information and audit rights

88. In-Scope Entities shall ensure within the written outsourcing *agreement* that the internal audit function, *the statutory auditor and the competent authority have a guaranteed access to the information relating to the outsourced functions* using a risk-based approach *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 the service provider and, in the cases provided for in the applicable national law, have the power to perform on-site inspections of the service provider. The aforementioned opinion may, where appropriate, be based on the reports of the service provider's external auditor*. *The written outsourcing agreement shall also provide that the internal control functions have access to any documentation relating to the outsourced functions, at any time and without difficulty, to maintain these functions' continued ability to exercise their controls.*

89. Regardless of the criticality or importance of the outsourced function, the written outsourcing *agreement* shall refer to the information gathering and investigatory powers of competent authorities under *Articles 49, 53 and 59 LFS and Articles 31, 38 and 58-5 LPS* and*, where applicable,* resolution authorities *under Article 61(1) BRRD Law* with regard to service providers located in a Member State and shall also ensure those rights with regard to service providers located in third countries.

90. With regard to the outsourcing of critical or important functions, In-Scope Entities shall ensure within the written outsourcing agreement that the service provider grants them, *their statutory auditor* and their competent authority, including*, where applicable,* their resolution authority, and any other person appointed by them or the competent authority *or resolution authority*, the following:

a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and

b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), *including the possibility for the competent authority to communicate any observations made in this context to the In-Scope Entities*, to enable them to monitor the outsourcing arrangement and to ensure compliance with *the* applicable regulatory and contractual requirements;

91. For the outsourcing of functions that are not critical or important, In-Scope Entities shall ensure the access and audit rights as set out in point 90 *and sub-section 4.3.2.3*, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its

scalability, the potential impact on the continuous performance of its activities and the contractual period. In-Scope Entities shall take into account that functions may become critical or important over time.

92. In-Scope Entities shall ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, *their statutory auditors*, competent authorities or third parties appointed by them to exercise these rights.

93. In-Scope Entities shall exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.

94. Without prejudice to their final responsibility regarding outsourcing arrangements, In-Scope Entities may use:

a. pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;

b. third-party certifications and third-party or internal audit reports, made available by the service provider.

95. For the outsourcing of critical or important functions, In-Scope Entities shall assess whether third-party certifications and reports as referred to in point 94(b) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.

96. In-Scope Entities shall make use of the method referred to in point 94(b) only if they:

a. are satisfied with the audit plan for the outsourced function;

b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the In-Scope Entity and the compliance with relevant regulatory requirements;

c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

d. ensure that key systems and controls are covered in future versions of the certification or audit report;

e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);

f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and

h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.

97. In-Scope Entities shall, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.

98. Before a planned on-site visit, In-Scope Entities, auditors or third parties acting on behalf of the In-Scope Entity or of the competent authority shall provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

99. When performing audits in multi-client environments, care shall be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.

100. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the In-Scope Entity shall verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the In-Scope Entity reviewing third-party certifications or audits carried out by service providers.

Sub-section 4.3.2.4 Termination rights

101. The outsourcing *agreement* shall expressly allow the possibility for the In-Scope Entity to terminate the arrangement in accordance with applicable law, including in the following situations:

a. where the *service* provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;

b. where impediments capable of altering the performance of the outsourced function are identified;

c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);

d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and

e. where instructions are given by the In-Scope Entity's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the In-Scope Entity.

102. The outsourcing *agreement* shall facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the In-Scope Entity*, whenever the continuity or quality of the service provision are likely to be affected*. To this end, the written outsourcing *agreement* shall:

a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the In-Scope Entity, including the treatment of data;

b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions;

c. include an obligation of the service provider to support the In-Scope Entity in the orderly transfer of the function in the event of the termination of the outsourcing agreement; *and*

d. without prejudice to applicable law, include a commitment for the service provider to erase the data and systems of the In-Scope Entity within a reasonable timeframe when the contract is terminated.

103. The outsourcing arrangement shall not include any termination clause or service termination clause in case of bankruptcy, controlled management, suspension of payments, compositions and arrangements with creditors aimed at preventing bankruptcy or other similar proceedings. In particular, in the context of BRRD institutions, clauses triggering the termination or service termination because of resolution actions, reorganisation measures or a winding-up procedure as required in accordance with the BRRD Law are not allowed.

Section 4.3.3 Oversight of outsourced functions

104. In-Scope Entities shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including *that the continuity of the services provided under the arrangement and* the availability, integrity and security of data and information are ensured. Where the risk, nature or scale of an outsourced function has materially changed, In-Scope Entities shall reassess the criticality or importance of that function.

105. In-Scope Entities shall apply due skill, care and diligence when *planning, implementing,* monitoring and managing outsourcing arrangements.

106. In-Scope Entities shall regularly update their risk assessment in accordance with points 66 to 70 and shall periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.

107. In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.

108. In-Scope Entities shall ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by:

a. ensuring that they receive appropriate reports from service providers;

b. evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and

c. reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.

109. In-Scope Entities shall take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, In-Scope Entities shall follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, In-Scope Entities shall take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.

110. In-Scope Entities[32] shall inform the competent authority *with no delay* of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of their business activities, *to allow the competent authority to assess whether regulatory action is needed.*

Section 4.3.4 Exit plans

111. In-Scope Entities shall have a documented exit *plan* when outsourcing critical or important functions that is in line with their outsourcing policy*, exit strategies and* business continuity plans, taking into account at least the possibility of:

[32] *See also Circular CSSF 21/787.*

a. the termination of outsourcing arrangements;

b. the failure of the service provider;

c. the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;

d. material risks arising for the appropriate and continuous application of the function.

112. In-Scope Entities shall ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they shall:

a. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and

b. identify alternative solutions and develop transition plans to enable In-Scope Entities to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the In-Scope Entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.

113. When developing exit *plans*, In-Scope Entities shall:

a. define the objectives of the exit *plan*;

b. perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;

c. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;

d. define success criteria for the transition of outsourced functions and data; and

e. define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under points 104 to 110) including indicators based on unacceptable service levels that shall trigger the exit.

Part II – Requirements in the context of ICT outsourcing arrangements

114. The purpose of this Part is to define specific requirements applicable in the context of ICT outsourcing (cloud and non-cloud), and that shall be complied with in addition to the general requirements laid out in Part I of this Circular. The following provisions contribute to the sound and prudent management, the proper organisation of the In-Scope Entities and the preservation of information security of the In-Scope Entities[33].

115. The requirements set out in the present Part II do not apply to business process outsourcing (i.e. outsourcing arrangements that are not pure ICT outsourcing) even if the outsourcing arrangements themselves rely on ICT outsourcing i.e. underlying ICT systems form part of this business process outsourcing.

116. When ICT outsourcing, or at least one of the sub-contractors in case of sub-outsourcing, relies on a cloud computing infrastructure as defined in point 1, the In-Scope Entities shall comply with the requirements of points 114 to 119, as relevant, and chapter 2 of Part II only. In case of ICT outsourcing arrangements other than those relying on cloud computing infrastructure as defined in point 1, In-Scope Entities shall comply with the requirements of points 114 to 119, as relevant, and chapter 1 of Part II only.

117. In case of ICT sub-outsourcing, the requirements of this Part (as applicable in line with point 116) shall apply to the whole outsourcing chain.

118. In accordance with the principle of proportionality, an In-Scope Entity may, if evidenced by comprehensive and robust conclusions from the assessment of the criticality of functions and the risk analysis, justify not applying the requirements set out in the following points when the ICT outsourcing is not critical or important and is unlikely to become critical or important:

a. point 103: continuity in case of resolution or reorganisation or another procedure; and

b. point 112(b): transfer of services where the continuity of the provision of services is threatened.

[33] As required, inter alia, under Article 5(1a) LFS, Article 17 LFS and Article 11(2) 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.

119. In-Scope Entities are reminded that for all ICT outsourcing arrangements, they shall:

a. ensure that access to data and systems 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; and

b. ensure that access to data subject to professional secrecy are granted in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable.

Chapter 1. ICT outsourcing arrangements other than those relying on a cloud computing infrastructure

120. The requirements of points 59 and 60 apply to ICT outsourcing arrangements concerned by the present chapter.

Sub-chapter 1.1 Requirements applicable to In-Scope Entities other than Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad

121. Without prejudice to point 119 above, In-Scope Entities may outsource their ICT system management/operation services:

a. in Luxembourg[34], solely to a credit institution or a financial professional holding a support PFS authorisation in accordance with Article 29-3 LFS (IT systems and communication networks operators of the financial sector "OSIRC"); the unique exception allowed under article 1-1 (2) c) LFS is the recourse to an entity of the group to which the In-Scope Entity belongs and which exclusively deals with group transactions;

b. abroad, to any ICT service provider, including an entity of the group to which the In-Scope Entity belongs.

122. In-Scope Entities may outsource ICT services other than ICT system management/operation services to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41(2a) LFS or Article 30(2a) LPS where applicable, the service provider may have access to this data only if it is

[34] As per the LFS, the operation of ICT systems for credit institutions, professionals of the financial sector, payment institutions, e-money institutions, UCIs, pension funds, insurance undertakings or reinsurance undertakings established under Luxembourg law or foreign law is a regulated activity requiring an authorisation to be exercised in Luxembourg.

overseen, throughout its mission, by a person of the In-Scope Entity in charge of ICT.

Sub-chapter 1.2 Requirements applicable to Support PFS authorised under Articles 29-3, 29-5 and 29-6 LFS and their branches abroad

123. For the exclusive purpose of this sub-chapter, the following definitions apply:

a. Support PFS: an In-Scope Entity, including its branches, that is authorised to perform OSIRC[35] activities in accordance with Article 29-3 or PSDC[36] activities in accordance with Articles 29-5 or 29-6 LFS;

b. Own ICT systems[37] [38]: systems supporting the support PFS' organisation and administration; they are not proposed as a service to third parties and not used by the services proposed to third parties;

c. Client ICT systems: systems that fulfill the two following cumulative conditions:

   i. they partially or exclusively support the activities carried out for regulated financial sector clients of the support PFS, irrespective of whether they belong to the client or to the support PFS or where they are located; and

   ii. the support PFS is responsible to its client for their proper functioning.

124. Without prejudice to point 119 above, support PFS and their branches authorised as OSIRC in accordance with Article 29-3 LFS may partially outsource their ICT operator services, i.e. some management/operation services of client ICT systems[39] provided that the conditions of points 126 and 127 are fulfilled.

125. Without prejudice to point 119 above, support PFS and their branches authorised as PSDC in accordance with Articles 29-5 or 29-6 LFS may partially outsource the management/operation of the ICT systems supporting partially or exclusively the dematerialisation or conservation services they provide to regulated financial sector clients provided that the conditions of points 126 and 127 are fulfilled.

[35] IT systems and communication networks operators of the financial sector ("OSIRC").
[36] Dematerialisation and/or conservation service providers of the financial sector ("PSDC").
[37] The term "system" here may be limited to software if the service relates solely to software.
[38] For example (non-exhaustive list): accounting systems, staff and payment management of the support PFS; management systems for clients' orders, purchase management, client relationship management but also email servers, the internal files servers, internet website of the support PFS (not the one used for services provided to its clients), the personnel's workstations, document storage, VoIP telephony, etc.
[39] Such an outsourcing by an OSIRC is actually a sub-outsourcing from the perspective of In-Scope Entities outsourcing to this OSIRC.

126. The service provider for the outsourcing arrangements referred to in points 124 and 125 above shall be:

a. in Luxembourg[40], solely a credit institution or an entity that is authorised as support PFS in accordance with Article 29-3 LFS;
b. Abroad, any ICT service provider, including an entity of the group to which the support PFS belongs.

127. The outsourcing arrangements referred to in points 124 and 125 above shall be considered as critical or important and are prohibited if they do not comply with the following:

a. The service provision is complementary[41] and does not carve out the support PFS (or its branch as relevant) of its substance in line with point 7;
b. Support PFS and their branches have obtained the prior approval of all their concerned regulated financial sector clients;
c. If the service provider may have access to data subject to professional secrecy according to Article 41 LFS or Article 30 LPS where applicable, the support PFS and their branches have clearly informed and obtained the prior consent of their regulated financial sector clients;
d. Each year, the support PFS and their branches must provide the competent authority with their detailed oversight plan and exit plan ensuring compliance with sections 4.3.3 and 4.3.4 of this Circular;
e. Support PFS and their branches have obtained the prior approval of the competent authority for such outsourcing using the instructions and, where available, the forms on the CSSF website.

128. Without prejudice to points 59, 60 and 119 above, support PFS and their branches may outsource the management/operation services of their own ICT systems:

a. in Luxembourg, solely to a credit institution or an entity that is authorised as support PFS in accordance with Article 29-3 LFS;

b. abroad, to any ICT service provider, including an entity of the group to which the support PFS belongs.

129. The provision of ICT operation services on client ICT systems or on systems supporting PSDC activities, by branches of support PFS to their registered office,

[40] As per the LFS, the operation of ICT systems for credit institutions, professionals of the financial sector, payment institutions, e-money institutions, UCIs, pension funds, insurance undertakings or reinsurance undertakings established under Luxembourg law or foreign law is a regulated activity requiring an authorisation to be exercised in Luxembourg.
[41] An example of complementarity is the operation of a software by an OSIRC (or its branch as relevant) and the cascading operation of the underlying infrastructure by a service provider.

are prohibited if they do not comply with the relevant requirements listed in point 127.

130. Support PFS and their branches acting as OSIRC may, for their services as ICT operators, rely on infrastructures belonging to their group, subject to the condition that the services provided by the group or their sub-contractors, if any, are limited to those requiring a physical presence on these infrastructures. The management of systems containing data and processing to be carried out by the support PFS shall be excluded from such outsourcing. Infrastructure shall mean the IT resources that are necessary to host the systems and data under the management of the OSIRC. 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 of data subject to the professional secrecy according to Article 41 LFS or Article 30 LPS, where applicable, the support PFS shall obtain the approval of the regulated financial sector clients before outsourcing.

131. Branches of support PFS may propose services relying on an infrastructure established in the country in which they are established ("host country") to their regulated financial clients in the host country. This infrastructure may be outsourced to a local service provider, subject to the condition that the services provided by this service provider and its sub-contractors, 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 oversight of the services provided by its branch. The branches shall obtain approval for this local outsourcing from their regulated financial sector clients concerned.

132. Support PFS may outsource any ICT services other than those covered by points 124 to 131 above to any ICT service provider, including a group entity providing ICT services or a support PFS. Such outsourcing arrangements must be set up in compliance with the requirements of point 119 above. In particular, if the service provider is not allowed to access to data subject to professional secrecy in compliance with Article 41 LFS or Article 30 LPS where applicable, the service provider may have access to this data only if it is overseen, throughout its mission, by a person of the Support PFS in charge of ICT.

Chapter 2. ICT outsourcing arrangements relying on a cloud computing infrastructure

133. This present chapter provides additional specific requirements to comply with in case of ICT outsourcing relying on a cloud computing infrastructure (hereafter also "cloud computing solution"). The use of a private cloud without outsourcing is thus excluded from the scope of this chapter.

Sub-chapter 2.1 Definitions and application

Section 2.1.1 Specific terminology

134. For the purposes of this chapter and in addition to definitions provided in point 1, the following definitions shall apply:

1) Client interface	the software layer made available by the cloud computing service provider to the In-Scope Entity allowing the latter to manage its cloud computing resources.
2) Cloud computing resource	any computing capabilities (e.g. server, storage, network, etc.) provided by a cloud computing service provider.
3) Cloud computing service provider	any firm proposing cloud services within the meaning of the definition of this chapter 2.
4) In-Scope Entity	an In-Scope Entity as defined in point 2, is consuming Cloud computing resources for the purpose of carrying out its activities.
5) Multi-tenant	a physical or logical infrastructure serving several (In-Scope) Entities through shared cloud computing resources and by means of a standardised model.
6) Resource operation	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.

Section 2.1.2 Definition of "cloud computing"

135. Cloud computing is a model composed of the following five essential characteristics[42]:

a. On-demand self-service: An In-Scope Entity[43] can unilaterally provide 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 (In-Scope) Entities using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to In-Scope Entity demand. There is a sense of location independence in that the In-Scope Entity 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 In-Scope Entity, 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 In-Scope Entity of the utilised service.

[42] The CSSF relies on the definitions proposed by international organisations such as the National Institute of Standards and Technology (NIST) or the European Union Agency for Cybersecurity (ENISA).

[43] For the sake of clarity, the definition considers the case where the In-Scope Entity itself is the operator of the resources used.

Section 2.1.3 Conditions of application of chapter 2

136. An outsourcing is considered as "outsourcing to a cloud computing infrastructure" within the meaning of this Circular and governed by the requirements of this chapter 2 if the five essential characteristics defined in point 135 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 In-Scope Entity owns on a cloud computing infrastructure without prior and explicit agreement of the In-Scope Entity and without monitoring mechanism available to the In-Scope Entity to control the accesses. These accesses must remain exceptional. Nevertheless, access may be necessary under a legal requirement or in an extreme emergency following a critical incident affecting part of or all the (In-Scope) Entities of the cloud computing service provider[44]. 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 In-Scope Entity[45] (e.g. provisioning, configuration or release of cloud computing resources). Thus, the resource operator alone (i.e. either the In-Scope Entity or a third party other than the cloud computing service provider) shall manage its ICT environment hosted on the cloud computing infrastructure. However, the cloud computing service provider may intervene manually:

   i. for global management of ICT systems supporting the cloud computing infrastructure (e.g. maintenance of physical equipment, deployment of new solutions non specific to the In-Scope Entity); or

   ii. within the context of a specific request by the In-Scope Entity (e.g. provisioning of a cloud computing resource that is missing in the catalogue proposed by the cloud computing service provider or performing insufficiently).

[44] In cases of extreme emergency, the In-Scope Entity should be informed a posteriori.
[45] Indeed, it is an automated system that allows provisioning resources, hence point (a) specifying that staff may not have access by default to In-Scope Entity resources.

Sub-chapter 2.2 Requirements to be observed with respect to outsourcing to a cloud computing infrastructure

137. In accordance with the principle of proportionality, the In-Scope Entity may, if evidenced by comprehensive and robust conclusions from the assessment of the criticality and importance of functions and the risk analysis, justify not to apply the requirements set out in the following points of this Circular when the activities outsourced to a cloud computing infrastructure are not related to a critical or important function and are unlikely to become critical or important:

a. point 142 c.: notification by the cloud computing service provider in case of change of functionalities;

b. point 142 d.: notification by the resource operator in case of change of functionalities;

c. point 143 a.: outsourcing agreement;

d. point 143 b.: resiliency of the services in the EEA.

138. The In-Scope Entity may outsource the "resource operation" as defined in point 134 to a third party when this third party falls under one of the following two circumstances:

a. The third-party is authorised as OSIRC under Article 29-3 LFS. The support PSF shall also comply with the requirements of this chapter where the operation of resources is carried out for an entity which is not a regulated financial sector client.

b. The third-party is not authorised as OSIRC under Article 29-3 LFS, either because it is located abroad, or because it is a Luxembourg-based entity of the group to which the In-Scope Entity belongs which provides operating services exclusively within the group as stated under the Article 1-1(2)c LFS. In such a case, in addition to complying with the requirements set out in this Circular, the In-Scope Entity shall perform a prior thorough risk analysis of the activities of the resource operator, notably by verifying that the following points have been correctly addressed:

   i. the roles and responsibilities defined between the resource operator and the cloud computing service provider;

   ii. the management of the isolation of multi-tenant environments;

   iii. the indicators collected by the resource operator to monitor the systems and data on the cloud computing infrastructure;

   iv. 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;

v. 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;

vi. the competences of the operators (e.g. certifications, technical training);

vii. the review of the audit reports of the cloud computing service provider by the resource operator;

viii. the competent authority's and the In-Scope Entity's right to audit the resource operator (in line with the requirements under points 88 to 100).

139. It shall be noted that an In-Scope Entity relying on a service provider that cumulates the activities of cloud computing service provider and resource operator is subject to the requirements of this chapter 2 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 definition of cloud computing within the meaning of this chapter). The same applies where the service provider cumulating both functions is authorized under Article 29-3 LFS. If this segregation requirement cannot be fulfilled, the outsourcing is not considered as an outsourcing to a cloud computing infrastructure within the meaning of this chapter but as a traditional ICT outsourcing; in such a case only the requirements of chapter 1 of Part II shall apply.

140. **Cloud Officer:**

a. 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 142a). 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 up by persons that already cumulate other functions within the ICT department.

b. If resource operation is performed by the In-Scope Entity, the "cloud officer" may cumulate the responsibility for the outsourcing relationship management. If the In-Scope Entity relies on a third party for cloud computing resource operation, the In-Scope Entity must know the name of the "cloud officer" of the resource operator.

141. **Necessity to inform the competent authority:**

a. The notification requirements of points 59 and 60 also apply to cloud computing outsourcing arrangements. In the particular case where an entity authorised under Article 29-3 LFS acts as an intermediary and not as a resource operator between an In-Scope Entity and a cloud computing

service provider, the In-Scope Entity shall submit a notification at least three (3) months before the planned outsourcing is effectively implemented for the outsourcing of critical or important functions to the cloud computing service provider.

b. Any entity authorised as OSIRC under Article 29-3 LFS shall request authorisation from the competent authority before marketing in the following cases:

   i. the entity intends to act as a resource operator for its regulated financial sector clients;

   ii. the entity intends to provide a cloud computing infrastructure to its regulated financial sector clients, acting thus as a cloud computing service provider;

   iii. the entity intends to provide a cloud computing solution to its regulated financial sector clients by relying on one or more cloud computing infrastructures. This entity acts then as a sub-outsourcing cloud computing service provider.

c. Without prejudice to point 119, support PFS and their branches authorised as OSIRC under Article 29-3 LFS may partially outsource their resource operator services[46] only under the conditions that compliance with point 126 and the requirements listed under point 127 are fulfilled. For the sake of clarity, a prior approval by the competent authority is therefore required as indicated in point 127 e. Point 129 also applies mutatis mutandis for the provision of resource operator services.

142. **Management of outsourcing risks:**

a. In line with point 35, 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", 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;

b. As set out in points 66 to 70, a risk assessment of outsourcing arrangements shall be carried out by the In-Scope Entity. The risks specific to the use of cloud computing technologies shall also be part of this assessment and encompass, e.g.: isolation failure in multi-tenant

[46] Such an outsourcing by an OSIRC is actually a sub-outsourcing from the perspective of In-Scope Entities outsourcing to this OSIRC.

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"[47], the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of continuity of cloud computing services;

c. Any change in the application functionality by the cloud computing service provider - other than the changes relating to corrective maintenance - shall be communicated prior to its implementation to the resource operator who shall inform the In-Scope Entity, so that they may take the necessary measures in case of material change or discontinuity;

d. Any change in the application functionality managed by the resource operator - other than the changes relating to corrective maintenance - shall be communicated to the In-Scope Entity, prior to its implementation, so that the latter may take the necessary measures in case of material change or discontinuity;

e. The In-Scope Entity and the resource operator shall have full awareness of the continuity and security elements remaining under their responsibilities when using a cloud computing solution;

f. The In-Scope Entity shall understand and the resource operator shall control the risks linked to a cloud computing infrastructure;

g. The In-Scope Entity and the resource operator shall know at any time where their data and systems are located globally[48], be it production environments or replications or backups.

143. **Contractual clauses:**

a. The outsourcing agreement signed with the cloud computing service provider shall be subject to the law of one of the Member States of the EEA. In the case where the outsourcing agreement signed is a group contract aiming at allowing the In-Scope Entity as well as other entities of the group to benefit from the cloud computing services, the contract may also be subject to the law of the country of the signing group entity, including when this country is outside the EEA.

b. The outsourcing agreement signed with the cloud computing service provider shall provide for a resiliency of the cloud computing services provided to the In-Scope Entity in the EEA. In this way, in case of spread

[47] "Shadow IT" is the use of ICT resources that is non-controlled by the ICT department.
[48] It is important that the In-Scope Entity 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 any circumstances.

of processing, data and systems over different data centres worldwide, at least one of the data centres shall be located in the EEA 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 In-Scope Entity. If all data centres backing the cloud computing services are located within the EEA, the resiliency requirement for the cloud computing services in the EEA is by default fulfilled. In the case where the outsourcing agreement signed is a group contract aiming at allowing the In-Scope Entity as well as other entities of the group outside of the EEA to benefit from the cloud computing services, the resiliency in the EEA is not mandatory but recommended and should be considered in the In-Scope Entity's risk analysis.

c. The In-Scope Entity may submit as part of its notification a request for a specific derogation to the competent authority where the requirements laid down in points a. and b. above cannot be fulfilled in case of an outsourcing of a critical or important function. This request shall be supported by detailed arguments justifying the use of this cloud computing service provider and stating precisely the resiliency measures planned in case of this service provider’s failure or failure of connections allowing access thereto.

Commission de Surveillance du Secteur Financier

Part III – Date of application

144. This Circular is applicable from *30 June 2022* to all outsourcing arrangements entered into, reviewed or amended on or after *this date*.

145. In-Scope Entities shall review and amend existing outsourcing arrangements with a view to ensuring that they are compliant with this Circular.

146. In-Scope Entities shall complete the documentation of all existing outsourcing arrangements in line with this Circular following the first renewal date of each existing outsourcing arrangement, but by no later than *31 December 2022.*

Where *the In-Scope Entities assess that* the review *and amendment of* outsourcing arrangements of critical or important functions *existing prior to 30 June 2022 will* not be finalised by *31 December 2022, they* shall inform their competent authority *in a timely manner* of that fact, including the measures planned to complete the review or the possible exit strategy.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex – List of implemented ESAs Guidelines

This Circular implements:

- the revised EBA Guidelines on outsourcing arrangements (**EBA/GL/2019/02)**;
- the ESMA Guidelines on outsourcing to cloud service providers (**ESMA50-164-4285**, the **ESMA Cloud Guidelines**) previously implemented by the Circular CSSF 21/777 amending the Circular CSSF 17/654.

The above-mentioned guidelines are available on the websites of the EBA (www.eba.europa.eu) and ESMA (www.esma.europa.eu).

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