Commission de Surveillance
du Secteur Financier

Circular CSSF 26/915

amending Circulars CSSF 20/750, 22/806, 25/881, 25/882, 25/883, 25/892 and 25/893

on the applicability of the Digital Operational Resilience Act (DORA) to third-country branches in Luxembourg

Circular CSSF 26/915

amending Circulars CSSF 20/750, 22/806, 25/881, 25/882, 25/883, 25/892 and 25/893

on the applicability of the Digital Operational Resilience Act (DORA) to third-country branches in Luxembourg

To all financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector[1] (DORA).

To all third-country branches of financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of DORA, if in the third country where their head office is established, they would qualify as entities listed under Article 2(1) (a) to (t) of DORA.

To all support PFS and specialised PFS within the meaning of the Law of 5 April 1993 on the financial sector (LFS).

To POST Luxembourg governed by the Law of 15 December 2000 on postal financial services and in its role as Payment Service Provider as referred to in Article 1(37) of the Law of 10 November 2009 on payment services (LPS).

To all management companies authorised only under Article 125-1 of Chapter 16 of the Law of 17 December 2010 relating to undertakings for collective investment (UCITS Law).

Luxembourg, 27 August 2026

Ladies and Gentlemen,

As of 17 January 2025, the provisions of DORA are applicable to the financial entities as defined in DORA and supervised by the CSSF. To fully reflect DORA provisions across the regulatory governance landscape of all regulated entities various CSSF circulars were updated, respectively published.

On 17 December 2025, the European Commission confirmed that DORA is also applicable to third-country branches (TCBs) in an EU country, if in the third country where their head office is established, they would qualify as entities listed under Article 2(1)(a) to (t) of DORA[2]. Consequently, an update of a series of circulars published or modified in 2025 is required to include TCBs in the DORA scope. Furthermore, the CSSF included in the frame of this update a precision regarding the reporting of major ICT-related incidents and cyber threats in case entities cannot use the prescribed communication channel.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

[2] Refer to DORA Q&A 102: DORA102 - 3097 - European Insurance and Occupational Pensions Authority

TABLE OF CONTENTS

Chapter 1: Scope

The following entities are to be considered as financial entities in the framework of this circular:

(a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements with a derogation and authorised reporting mechanisms with a derogation within the meaning of the LFS;
(b) payment institutions, account information service providers and electronic money institutions within the meaning of the LPS;
(c) crypto asset service providers and issuers of asset-referenced tokens within the meaning of Regulation (EU) 2023/1114;
(d) central securities depositories within the meaning of the Law of 6 June 2018 on central securities depositories;
(e) central counterparties within the meaning of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories;
(f) management companies incorporated under Luxembourg law and subject to Chapter 15 or Article 125-2 of Chapter 16, and Luxembourg branches of investment fund managers subject to Chapter 17, and investment companies which did not designate a management company within the meaning of Article 27 of the UCITS Law;
(g) alternative investment fund managers authorised under Chapter 2 and internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the Law of 12 July 2013 on alternative investment fund managers;
(h) institutions for occupational retirement provisions authorised in accordance with Article 2(2) of the Law of 13 July 2005 on institutions for occupational retirement provision in the form of pension savings companies with variable capital (SEPCAVs) and pension savings associations (ASSEPs);
(i) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of Regulation (EU) 2016/1011;
(j) crowdfunding service providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;
(k) Payment Service Providers (PSPs) as referred to in Article 1(37) of the LPS that are not financial entities as defined in points (a) and (b) above, i.e. POST Luxembourg;
(l) third-country branches of undertakings listed under points (a) to (j) above and having their head office in a third country that would qualify under Article 2(1) (a) to (i), (k) to (m), (p), (r) and (s) of DORA;
(m) support PFS and specialised PFS within the meaning of the LFS;
(n) management companies authorised only under Article 125-1 of Chapter 16 of the UCITS Law.

Chapter 2: Applicability to Third-Country Branches (TCBs) under DORA

EIOPA has relayed the European Commission's response under Question ID "DORA102 – 3097" stating that Regulation (EU) 2022/2554 (DORA) is applicable to TCBs in an EU country.

The CSSF is giving effect to this stance via this Circular. TCBs of undertakings having their head office in a third country and that would qualify under Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of DORA, are in the context of this circular and all amended circulars, as per the list below, to be considered as financial entities subject to DORA.

The following modifications have been made to the enumerated circulars:

1. Removal of TCBs from the scope of the following circulars (or part thereof):
   - *Circular CSSF 20/750 – Requirements regarding information and communication technology (ICT) and security risk management*: full removal.
   - *Circular CSSF 22/806 – on outsourcing arrangements*: The application of the circular for ICT outsourcing (Part II) was removed but kept for outsourcing arrangements other than ICT (Part I), in full alignment with other DORA entities.

2. Inclusion of TCBs in the scope of the following circulars applicable to DORA entities:
   - *Circular CSSF 25/882 - on requirements on the use of ICT third-party services for Financial Entities subject to the Digital Operational Resilience Act (DORA)*.
   - *Circular CSSF 25/892 - Application of the Joint ESA Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)*.
   - *Circular CSSF 25/893 - on reporting of major ICT-related incidents and significant cyber threats under the Digital Operational Resilience Act (DORA).* Note that point 9 was also modified to introduce an alternative communication channel in case of technical impossibility preventing financial entities to notify the CSSF of major ICT related incidents and/or cyber threats via the indicated primary channel.

3. To avoid inconsistencies and align with the above changes, modification of the two "amending circulars" which were used to modify the "pre-DORA CSSF circulars" when DORA entered into application:
   - *Circular CSSF 25/881 – amending Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management*: In line with above, TCBs were removed from the amendment of Circular CSSF 20/750.
   - *Circular CSSF 25/883 - amending Circular CSSF 22/806 on outsourcing arrangements*: Alignment of the modification of Circular CSSF 22/806 above.

To visualise the respective changes, the corresponding pages of the amended Circulars are annexed to this Circular in track changes.

Chapter 3: Date of application

This circular shall apply with immediate effect.

Pascale TOUSSING
Director

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Claude MARX
Director General

Annexes

Circular CSSF 20/750 as amended by Circular CSSF 26/915

Circular CSSF 22/806 as amended by Circular CSSF 26/915

Circular CSSF 25/881 as amended by Circular CSSF 26/915

Circular CSSF 25/882 as amended by Circular CSSF 26/915

Circular CSSF 25/883 as amended by Circular CSSF 26/915

Circular CSSF 25/892 as amended by Circular CSSF 26/915

Circular CSSF 25/893 as amended by Circular CSSF 26/915

Commission de Surveillance
du Secteur Financier

Circular CSSF 20/750

as amended by Circulars CSSF 22/828, CSSF 25/881 and CSSF 26/915

on requirements regarding information and communication technology (ICT) and security risk management

Circular CSSF 20/750

as amended by Circulars CSSF 22/828, CSSF 25/881 and CSSF 26/915

on requirements regarding information and communication technology (ICT) and security risk management

To support PFS and specialised PFS within the meaning of the Law of 5 April 1993 on the financial sector (LFS), and POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[1]~~., as well as to all branches in Luxembourg of credit institutions, investment firms, payment institutions and e-money institutions incorporated in a third country~~

Luxembourg, 25 August 2020

Ladies and Gentlemen,

This circular reflects the expectations of the CSSF as regards the risk management measures and control and security arrangements as referred to in Articles 17(1a) and 36(1) of the Law of 5 April 1993 on the financial sector ("LFS") and in Article 105-1 (1) of the Law of 10 November 2009 on payment services ("LPS").

This circular is divided in four Chapters:

- Chapter 1 indicates the scope of this circular
- Chapter 2 provides definitions and clarifications with regards to the terms used in this circular
- Chapter 3 lists the requirements regarding ICT and security risk management
- Chapter 4 indicates the entry into force of this circular

[1] *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.*

TABLE OF CONTENTS

Chapter 1. Entities in Scope

This circular is applicable in full to all the following entities:

a) All support PFS within the meaning of the Law of 5 April 1993 on the financial sector (LFS)

b) All specialised PSF within the meaning of the Law of 5 April 1993 on the financial sector (LFS)

c) POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[2] and as Payment Service Provider as referred to in Article 1(37)(iii) of the LPS

~~d) All branches in Luxembourg of credit institutions incorporated in a third country~~

~~e) All branches in Luxembourg of investment firms incorporated in a third country~~

~~f) All branches in Luxembourg of payment institutions and electronic money institutions incorporated in a third country~~

Chapter 2. Definitions

Financial Institution	Throughout this document this term refers to the supervised entities in scope of this circular as defined in Chapter 1.
Payment Service Provider (PSP)	Throughout this document this term refers to POST Luxembourg~~ and branches in Luxembourg of credit institutions, payment institutions and electronic money institutions incorporated in a third country, when they provide payment services as defined in Article 1(38) of the LPS~~.
ICT and security risk	Risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.
Management body	A Financial Institution's body or bodies, which are appointed in accordance with national law, which are empowered to set the Financial Institution'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 Financial Institution and the directors and persons responsible for the management of the Financial Institution.

[2] *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.*

	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.
Operational or security incident	A singular event or a series of linked events unplanned by the financial institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.
Risk appetite	The aggregate level and types of risk that the PSPs and institutions are willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives.
ICT projects	Any project, or part thereof, where ICT systems and services are changed, replaced, dismissed or implemented. ICT projects can be part of wider ICT or business transformation programmes.
Third party	An organisation that has entered into business relationships or contracts with an entity to provide a product or service.
Information asset	A collection of information, either tangible or intangible, that is worth protecting.
ICT asset	An asset of either software or hardware that is found in the business environment.
ICT systems	ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial institution.
ICT services	means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services. [3]

[3] Definition from Article 3(21) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("DORA")

Chapter 3. Guidelines on ICT and security risk management

3.1. Proportionality

1. All financial institutions should comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, the financial institutions' size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.

3.2. Governance and strategy

3.2.1. Governance

2. The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.
3. The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7.)
4. The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

3.2.2. Strategy

5. The ICT strategy should be aligned with financial institutions' overall business strategy and should define:
    a. How financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;
    b. The planned strategy and evolution of the architecture of ICT, including third-party dependencies;
    c. Clear information security objectives, focusing on ICT systems and ICT services, staff and processes
6. Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and third-party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial

institutions should also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy.

3.2.3. Use of third-party providers

7. Without prejudice to Circular CSSF 22/806 on outsourcing arrangements, financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.
8. To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption- see also section 3.7.2.) with providers (outsourcing providers, group entities, or third-party providers) include the following:
    a. Appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;
    b. Operational and security incident handling procedures including escalation and reporting.
9. Financial institutions should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets of the financial institution.

3.3. ICT and security risk management framework

3.3.1. Organisation and objectives

10. Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.
11. Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function. Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit.

    The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institutions with the financial institution's policies and procedures and with external requirements.

12. Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.

13. The ICT and security risk management framework should include processes in place to:

    a. Determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution;
    b. Identify and assess the ICT and security risks to which a financial institution is exposed;
    c. Define mitigation measures, including controls, to mitigate ICT and security risks;
    d. Monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 105-2 of LPS affecting the ICT-related activities, and take action to correct the measures where necessary;
    e. Report to the management body on the ICT and security risks and controls;
    f. Identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.

14. Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on "lessons learned" during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.

3.3.2. Identification of functions, processes and assets

15. Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

16. In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.

3.3.3. Classification and risk assessment

17. Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.

18. To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.

19. Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.

20. Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter

intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.

21. Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.

3.3.4. Risk mitigation

22. Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. A financial institution should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the financial institution's ICT and security risk appetite.

23. Financial institutions should define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.

3.3.5. Reporting

24. Financial institutions should report risk assessment results to the management body in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 105-1(2) of LPS.

3.3.6. Audit

25. A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

26. A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.

27. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.

3.4. Information security

3.4.1. Information security policy

28. Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' data and information. The information security policy should be in line with the financial institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.

29. The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial institution.

30. Based on the information security policy, financial institutions should establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures should include:

    a. organisation and governance in accordance with paragraphs 10 and 11;
    b. logical security (Section 3.4.2);
    c. physical security (Section 3.4.3);
    d. ICT operations security (Section 3.4.4);
    e. security monitoring (Section 3.4.5);
    f. information security reviews, assessment and testing (Section 3.4.6);
    g. information security training and awareness (Section 3.4.7).

3.4.2. Logical security

31. Financial institutions should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also includes technical users:

    a. **Need to know, least privilege and segregation of duties:** financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

b. **User accountability:** financial institutions should limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.

c. **Privileged access rights:** financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.

d. **Logging of user activities:** at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.

e. **Access management:** access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.

f. **Access recertification:** access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.

g. **Authentication methods:** financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

32. Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service.

3.4.3. Physical security

33. Financial institutions' physical security measures should be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

34. Physical access to ICT systems should be permitted to only authorised individuals. Authorisation should be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

35. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

3.4.4. ICT operations security

36. Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:

    a. identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;
    b. implementation of secure configuration baselines of all network components;
    c. implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);
    d. implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;
    e. ensuring that mechanisms are in place to verify the integrity of software, firmware and data;
    f. encryption of data at rest and in transit (in accordance with the data classification).

37. Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.

3.4.5. Security monitoring

38. Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact financial institutions' information security and to respond to these events appropriately. As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover:

    a. relevant internal and external factors, including business and ICT administrative functions;
    b. transactions to detect misuse of access by third parties or other entities and internal misuse of access;
    c. potential internal and external threats.

39. Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.

40. The security monitoring process should also help a financial institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.

3.4.6. Information security reviews, assessment and testing

41. Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team exercises.

42. Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

43. The information security testing framework should ensure that tests:

    a. are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;
    b. include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

44. Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 105-1(2) of LPS. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.

45. Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

46. Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.

47. For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

48. Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

3.4.7. Information security training and awareness

49. Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.

3.5. ICT operations management

50. Financial institutions should manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body[4]. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.

51. Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

52. Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.

53. Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.

54. The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.

55. Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.

56. Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

57. Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the

[4] means "management body or authorised management as defined by the management body"

data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

58. Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

3.5.1. ICT incident and problem management

59. Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this circular, as well as early warning indicators that should serve as alerts to enable early detection of these incidents.
60. To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process should establish:

    a. the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;
    b. the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);
    c. problem management procedures to identify, analyse and solve the root cause behind one or more incidents — a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and should consider key lessons learned from these analyses and update the security measures accordingly;
    d. effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints — to ensure that:
        i. incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management[5] and ICT senior management[6];
        ii. the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.
    e. incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;
    f. specific external communication plans for critical business functions and processes in order to:
        i. collaborate with relevant stakeholders to effectively respond to and recover from the incident;

[5] means "management"

[6] means "management"

ii. provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.

3.6. ICT project and change management

3.6.1. ICT project management

61. A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

62. A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

63. A financial institution should establish and implement an ICT project management policy that includes as a minimum:

    a. project objectives;
    b. roles and responsibilities;
    c. a project risk assessment;
    d. a project plan, timeframe and steps;
    e. key milestones;
    f. change management requirements.

64. The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.

65. A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

66. The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.

3.6.2. ICT systems acquisition and development

67. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.

68. A financial institution should ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.

69. A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

70. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.

71. Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

72. A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.

73. Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

74. A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.

3.6.3. ICT change management

75. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

76. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.

3.7. Business continuity management

77. Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption.

3.7.1. Business impact analysis

78. As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third-party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3.

79. Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

3.7.2. Business continuity planning

80. Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

81. Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.

82. A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.

3.7.3. Response and recovery plans

83. Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.

84. The response and recovery plans should consider both short-term and long-term recovery options. The plans should:

    a. focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;
    b. be documented and made available to the business and support units and readily accessible in the event of an emergency;
    c. be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

85. The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

86. Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third-party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the Circular CSSF 22/806 on outsourcing arrangements regarding business continuity plans).

3.7.4. Testing of plans

87. Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.

88. BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.

89. Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. In particular they should:

    a. include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;

    b. be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and

    c. include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 89(a).

90. Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.

3.7.5. Crisis communication

91. In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing providers, group entities, or third-party providers) are informed in a timely and appropriate manner.

Chapter 4. Date of application

92. This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Commission de Surveillance
du Secteur Financier

Circular CSSF 22/806

as amended by Circulars CSSF 25/883 and 26/915

on outsourcing arrangements

Circular CSSF 22/806

as amended by Circulars CSSF 25/883 and 26/915

on outsourcing arrangements

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 management companies authorised only under Article 125-1 of Chapter 16 of the Law of 17 December 2010 relating to undertakings for collective investment (UCITS Law)

Luxembourg, 22 April 2022

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.

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.

As of 17 January 2025, the provisions of the Digital Operational Resilience Act (**DORA**), Regulation (EU) 2022/2554, apply to all financial entities as defined under Article 2(1), points (a) to (t) of DORA. This circular has therefore been amended in order to provide legal clarity to the market and to avoid duplication of requirements with the provisions set forth in DORA. This alignment reflects the CSSF's continued commitment to ensuring the effective management of ICT third-party risks within the financial sector while adhering to evolving European regulatory frameworks.

TABLE OF CONTENTS

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.*

[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.

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.*
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.

[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.

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) DORA	*Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*
21) EBA	*the European Banking Authority*
22) ECB	*European Central Bank*
23) EEA	*European Economic Area*
24) ESMA	*the European Securities and Markets Authority*
25) 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)*
26) ICT	*Information and Communication Technology*

27) LFS	*Law of 5 April 1993 on the financial sector, as amended*
28) LPS	*Law of 10 November 2009 on payment services, as amended*
29) 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*
30) MiFID Law	*Law of 30 May 2018 on markets in financial instruments, as amended*
31) 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.

Part I of this circular applies to the following In-Scope Entities when performing outsourcing other than ICT outsourcing[6]:

- credit institutions[7] [8], including their branches, within the meaning of the LFS;

- investment firms, including their branches, within the meaning of the LFS;

*- payment institutions and electronic money institutions, including their branches, (each referred to as a **payment institution**) within the meaning of the LPS. 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;*

- branches in Luxembourg of credit institutions, investment firms and payment institutions incorporated in a third country. They shall be deemed to be included in the notion of credit institution, investment firm and payment institution respectively.

This circular applies in full (Part I and Part II) to the following In-Scope Entities:

*- specialised and support 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[9]. All provisions that apply to payment institutions shall also apply to POST Luxembourg.

[6] For the sake of clarity, these entities are not required to include their ICT outsourcing arrangements in the register referred to in section 4.2.7.
[7] 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).
[8] 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.
[9] 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.

~~*- branches in Luxembourg of credit institutions, investment firms and payment institutions incorporated in a third country. They shall be deemed to be included in the notion of credit institution, investment firm and payment institution respectively.*~~

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

- management companies authorised only under Article 125-1 of Chapter 16 of the UCITS Law

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[10], Part I of this circular applies if EEA branches outsource functions that belong to areas for which the CSSF retains an oversight responsibility, except for ICT outsourcing[11]. While this circular does not impose specific requirements with regard 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, well integrated and *appropriate* for the effective application of this circular at all relevant levels *of supervision*[12].

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.*

[10] 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.

[11] Those arrangements are covered by Circular CSSF 25/882 on requirements on the use of ICT third-party services for Financial Entities subject to DORA and DORA regulation.

[12] 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.

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.

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[13], card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).

[13] 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.

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[14] 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 concerns functions related to core business lines and critical functions *according to the BRRD Law*[15] and identified by these institutions using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778[16]. 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;

[14] See the activities listed in Annex I of LFS and in Annex of LPS related to payment services.
[15] *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.*
[16] 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.

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;

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[17].

[17] 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.

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,[18] 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.[19]

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.

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,

[18] *Please also refer to Articles 6, 7, 24-2 and 24-3 LPS, when applicable.*
[19] *Please refer to Circular CSSF 20/750 on ICT and security risk management.*

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*[20] shall at least ensure a clear *and sound* division of tasks and responsibilities for the management and control 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);

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

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"*[21].

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;

[21] 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[22]

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

[22] 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.

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 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[23], 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;

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

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 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[24] 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

[24] 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.

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.

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[25], 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[26] 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[27].

[25] 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.
[26] or POST Luxembourg.
[27] 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.

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.

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[28], 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.

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

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;

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[29] powers, especially to Articles 59-47 LFS, 66 and 69 of the BRRD Law, and in particular a description

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

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.

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;[30]

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

[30] Please refer to Article 28 GDPR.

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 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 142.*

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[31] 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:

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.

[31] See also Circular CSSF 21/787.

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[32].

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.

[32] 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.

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.

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[33], 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

[33] 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.

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 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[34] activities in accordance with Article 29-3 or PSDC[35] activities in accordance with Articles 29-5 or 29-6 LFS;

b. Own ICT systems[36] [37]: 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[38] 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

[34] IT systems and communication networks operators of the financial sector ("OSIRC").
[35] Dematerialisation and/or conservation service providers of the financial sector ("PSDC").
[36] The term "system" here may be limited to software if the service relates solely to software.
[37] 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.
[38] Such an outsourcing by an OSIRC is actually a sub-outsourcing from the perspective of In-Scope Entities outsourcing to this OSIRC.

provide to regulated financial sector clients provided that the conditions of points 126 and 127 are fulfilled.

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

a. in Luxembourg[39], 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[40] 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, 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

[39] 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.
[40] 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.

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 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[41]:

a. On-demand self-service: An In-Scope Entity [42] 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.

[41] 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 Network and Information Security (ENISA).

[42] 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[43]. 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[44] (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).

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.

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:

[43] In cases of extreme emergency, the In-Scope Entity should be informed a posteriori.
[44] 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.

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 authorised 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[45] 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 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

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

"shadow IT"[46], 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[47], be it production environments or replications or backups.

[46] "Shadow IT" is the use of ICT resources that is non-controlled by the ICT department.
[47] 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.

Part III. Date of application

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

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

145. 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 ESA Guidelines

Annex – List of implemented ESA 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 Circular CSSF 21/777 amending 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

Circular CSSF 25/881

as amended by Circular CSSF 26/915

amending Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management

Circular CSSF 25/881

as amended by Circular CSSF 26/915

amending Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management

To all credit institutions and to all professionals of the financial sector within the meaning of the Law of 5 April 1993 on the financial sector (LFS).
To POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[1].
To all payment institutions and to all electronic money institutions within the meaning of the Law of 10 November 2009 on payment services (LPS).

Luxembourg, 9 April 2025

Ladies and Gentlemen,

As of 17 January 2025, the provisions of the Digital Operational Resilience Act[2] ("DORA") are applicable to the financial entities as defined in DORA and supervised by the CSSF. DORA has introduced, inter alia, harmonised requirements for information and communication technology (ICT) risk management framework.

In view of reducing the overlap with the DORA regulation, the European Banking Authority ("EBA") reviewed its existing Guidelines on ICT and security risk management EBA/GL/2019/04 (the "EBA Guidelines"), which were built on the provisions of Article 74 of Directive 2013/36/EU (CRD)[3] and Article 95(3) of Directive (EU) 2015/2366 (Payment Services Directive 2, "PSD2")[4]. The EBA Guidelines are implemented in Luxembourg by way of Circular CSSF 20/750 on ICT and security risk management.

The EBA arrived at the view that the entities subject to the EBA Guidelines should be narrowed down and the scope of the Guidelines reduced to Guideline 3.8 on relationship management of the payment service users in relation to the provision of payment services. To do so, the EBA issued EBA GL 2025/02 amending EBA GL/2019/04 on ICT and security risk management ("new EBA Guidelines"). The EBA further explained that National Competent Authorities have the possibility to subject Payment Service Providers (PSPs) that are not covered by DORA to national requirements irrespective of the existence or not of EBA Guidelines[5].

[1] 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.

[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

[3] https://eur-lex.europa.eu/eli/dir/2013/36/oj/eng

[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35–127)

[5] EBA/GL/2025/02 and corresponding press release

Consequently, to provide legal clarity to the market and clarify its expectations, the CSSF is taking two steps:

1. amend Circular CSSF 20/750 on requirements regarding ICT and security risk management:
   - **to reduce the scope to "non-DORA entities", i.e. the entities that are subject to CSSF supervision but are not financial entities as defined in Article 2 of DORA** and therefore not subject to DORA requirements. The amended Circular CSSF 20/750 also remains applicable to entities which are not in the scope of DORA, when providing payment services, such as POST Luxembourg ~~and branches in Luxembourg of PSP incorporated in a third country~~[6]. In fact, the CSSF considers that financial entities subject to the supervision of the CSSF falling under Circular CSSF 20/750 but not falling under DORA shall continue to fulfil its expectations with regard to the ICT and security risk management by complying with this circular;
   - **to remove the specific elements only applicable to PSPs** (whether they are also in scope of DORA or not) which are regrouped in a new dedicated circular (see point 2 below), i.e. Guideline 3.8. on relationship management of the payment service users and section 4 of the circular related to PSP ICT assessment; and
   - to remove a few other obsolete sections and provisions of the circular.

2. issue a new circular, Circular CSSF 25/880 on relationship management of payment service users and PSP ICT assessment, **applicable to all PSPs** within the scope of LPS and supervised by the CSSF, including branches in Luxembourg of PSPs incorporated in a third country, and POST Luxembourg which:
   - **implements the EBA Guidelines 2025/02** amending EBA GL/2019/04 on ICT and security risk management. i.e. the contents of Guideline 3.8 referred to above;
   - **integrates** the existing additional national requirement for annual reporting of the risk assessment related to payment services (**PSP ICT assessment**), which was previously part of Circular CSSF 20/750.

In line with step 1 above, this circular amends Circular CSSF 20/750 by specifying the following:

1. the scope of application of Circular CSSF 20/750 has been modified to consider the entry into application of DORA. The scope is now described in Chapter 1:

   a. For financial entities as defined in Article 2 of DORA and supervised by the CSSF, Circular CSSF 20/750 no longer applies. They have been removed from the scope;

   b. For entities falling under Circular CSSF 20/750 but not falling under DORA, Circular CSSF 20/750 continues to apply in full.

2. Section 1 on "Requirements regarding information and communication technology (ICT) and security risk management", Section 2 on "Amendment of Circular CSSF 12/552", Section 3 on "Repeal and replacement of Circular CSSF 19/713" and Section 4 on "Additional requirement for payment service providers (PSPs)" have been removed.

3. The requirements that were listed in EBA Guidelines EBA/GL/2019/04 have been introduced directly in Circular CSSF 20/750 as follows:

[6] This is the reason why references to elements of compliance with the Law of 10 November 2009 on payment services (LPS) which apply to POST Luxembourg ~~and branches in Luxembourg of PSP incorporated in a third country~~ are retained in this circular.

a. The text of the EBA Guidelines in the section "Definitions" can now be found in Chapter 2;

b. The text of the EBA Guidelines in the section "Guidelines on ICT and security risk management" can now be found in Chapter 3.

The amendments to the EBA Guidelines, which are now in Chapters 2 and 3 are shown in track changes. They relate to requirements or references which were primarily relevant for entities which are now out of scope of this circular. In addition, some definitions were modified to align them with recent definitions in this area.

This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex Circular CSSF 20/750 as amended by Circular CSSF 25/881

Commission de Surveillance
du Secteur Financier

Circular CSSF 25/882

as amended by Circular CSSF 26/915

on requirements on the use of ICT third-party services for Financial Entities subject to the Digital Operational Resilience Act (DORA)

Circular CSSF 25/882

as amended by Circular CSSF 26/915

on requirements on the use of ICT third-party services for Financial Entities subject to the Digital Operational Resilience Act (DORA)

To all financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA~~"~~) [1].

To all third-country branches of financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of DORA, if in the third country where their head office is established, they would qualify as entities listed under Article 2(1) (a) to (t) of DORA.

Luxembourg, 9 April 2025

Ladies and Gentlemen,

As of 17 January 2025, the provisions of ~~the Digital Operational Resilience Act ("~~DORA~~") (Regulation (EU) 2022/2554)~~ are applicable to the financial entities supervised by the CSSF and in scope of DORA.

The purpose of this circular is to provide them with practical instructions on the submission of certain information and reporting in relation to the use of ICT third-party providers and required under DORA.

This circular also complements the DORA Regulation, notably by recalling certain general requirements regarding the use of ICT services[2] provided by third parties, considering notably the Luxembourg national laws related to financial services.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

[2] ICT services as defined in DORA Article 3(21)

TABLE OF CONTENTS

Chapter 1: Scope and general principles

Sub-chapter 1.1. Scope

1. The following entities are to be considered as financial entities in the framework ~~in the scope~~ of this circular:

   a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements with a derogation and authorised reporting mechanisms with a derogation within the meaning of the Law of 5 April 1993 on the financial sector (LFS);

   b) payment institutions, account information service providers and electronic money institutions within the meaning of the Law of 10 November 2009 on payment services (LPS);

   c) crypto asset service providers and issuers of asset-referenced tokens within the meaning of Regulation (EU) 2023/1114;

   d) central securities depositories within the meaning of the Law of 6 June 2018 on Central Securities Depositories;

   e) central counterparties within the meaning of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories;

   f) management companies incorporated under Luxembourg law and subject to Chapter 15 or Article 125-2 of Chapter 16, and Luxembourg branches of investment fund managers subject to Chapter 17, and investment companies which did not designate a management company within the meaning of Article 27 of the Law of 17 December 2010 relating to undertakings for collective investment;

   g) alternative investment fund managers authorised under Chapter 2 and internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the Law of 12 July 2013 on alternative investment fund managers;

   h) institutions for occupational retirement provisions authorised in accordance with Article 2(2) of the Law of 13 July 2005 on institutions for occupational retirement provision in the form of pension savings companies with variable capital (SEPCAVs) and pension savings associations (ASSEPs);

   i) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of Regulation (EU) 2016/1011;

   ~~j)~~ crowdfunding service providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;

   ~~j)~~k) third-country branches of undertakings listed under points 1.a) to j) above and having their head office in a third country that would qualify under Article 2(1) (a) to (i), (k) to (m), (p), (r) and (s) of DORA.

2. The provisions of this circular are applicable to all financial entities in scope as defined in point 1(a) to (k~~j~~) above, hereinafter collectively referred to as "**Financial Entities**" or individually as "**Financial Entity**", including their branches as specified in the respective laws.

3. For branches in Luxembourg of the Financial Entities that are part of a legal entity whose head office is located in a different Member State of the European Union (EU branches), Chapter 2: of this circular shall not apply.

4. For significant credit institutions, for which the ECB is the competent authority for the prudential supervision, Chapter 2: of this circular shall not apply.

Sub-chapter 1.2. Use of a third-party for ICT operation services

5. Financial Entities are reminded that for all arrangements on the use of ICT services provided by ICT third-party service providers, they shall 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.

6. Contractual arrangements with a third-party located in Luxembourg that relate to ICT services subject to an authorisation requirement in accordance with Article 29-3 LFS, i.e. ICT management/operations services (including resource operation services in case of use of cloud services[3]) to certain types of Financial Entities[4], shall take place only if one of the following conditions is met:

   a. the service provider is authorised by the CSSF in accordance with Article 29-3 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 Financial Entity belongs and which exclusively deals with group transactions.

7. Financial Entities may make contractual arrangements on the use of ICT services other than the ones covered under point 6 above, to any ICT service provider in Luxembourg or abroad. Such outsourcing arrangements must be set up in compliance with the requirements of point 5 above. In particular, if the service provider is not allowed 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 overseen, throughout its mission, by a person of the Financial Entity in charge of ICT.

Sub-chapter 1.3. Backup of accounting positions

8. When using an accounting system that is located outside of Luxembourg (accounting system hosting services) independently or in connection with the outsourcing of operational tasks of the accounting function, the Financial 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

[3] Reference is made to Chapter 3 of this circular for definitions of cloud services and resource operation.

[4] The types of Financial Entities are listed in Article 29(3) LFS.

format, to guarantee an autonomous preparation of a balance sheet, a profit and loss statement and client positions[5].

9. This backup shall be stored at the premises of the Financial Entity in Luxembourg, of a group entity located in the EEA, or of another service provider (i.e. a service provider different from the one that provides the accounting system hosting service) located in the EEA.

10. Financial Entities acting as UCI administrator in the meaning of Circular CSSF 22/811 shall apply the requirements of points 8 and 9 above considering point 80 of Circular CSSF 22/811 which contains similar requirements tailored to UCI administration activities.

Chapter 2: DORA reporting obligations

Sub-chapter 2.1. Notification of planned contractual arrangements regarding the use of ICT services supporting critical or important functions

11. In accordance with Article 28(3) of DORA, Financial Entities shall inform the competent authority in a timely manner about any planned contractual arrangement regarding the use of ICT services supporting critical or important functions as well as when a function has become critical or important.

12. This notification shall be made using the instructions and forms available on the CSSF website.

13. The notification is to be submitted at least three (3) months before the planned contractual arrangement comes into effect. When resorting to a Luxembourg support PFS governed by Articles 29-3, 29-5 or 29-6 LFS, this notice period is reduced to one (1) month. Any planned contractual arrangement which has not been notified within the above notification period and/or without using the instructions and forms available on the CSSF website will be considered as not notified.

14. 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 projects do not comply with the applicable legal and regulatory framework.

15. In any event, Financial Entities remain fully responsible to comply with all the relevant laws and regulations as regards the planned contractual arrangements regarding the use of ICT services.

[5] The aim of this requirement is to ensure that in case of sudden interruption of services provided by the service provider, the last positions are known and available to the Financial Entity in Luxembourg or in the EEA. The objective is not to ensure the continuity of the accounting function. The backup can therefore be a copy/picture e.g. via simple extraction from the system, of the accounting positions, including client positions.

Sub-chapter 2.2. Register of information

16. In accordance with Article 28(3) of DORA, Financial Entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

17. Financial Entities must submit annually to the CSSF their register at individual or consolidated level, when relevant[6], as further explained on the CSSF website.

18. The register of year n should contain all arrangements contracted until the end of year n and is to be submitted between 28 February and 31 March of year n+1 at the latest, following the instructions available on the CSSF website. By way of derogation[7], for the first year of collection (2025), the register should contain all arrangements contracted until 31 March 2025 and is to be submitted between 1 April 2025 and 15 April 2025.

19. After any request from the CSSF to correct any data in the register, Financial Entities shall promptly perform the requested correction and submit the corrected register to the CSSF.

20. Outside the official submission period defined in point 18 above, the CSSF reserves the right to request the register of information at any time.

Chapter 3: Use of ICT third-party cloud computing services

21. This chapter mainly provides clarifications on the definition of cloud computing and cloud services in case of use of ICT third-party cloud computing services, in order to fully identify and differentiate cloud computing from resource operation services. Indeed, as outlined in point 6 of this circular, in Luxembourg, resource operations services can only be delivered to certain types of Financial Entities by specific service providers.

Sub-chapter 3.1. Definitions related to cloud computing

3.1.1. Specific terminology

22. For the purposes of this chapter, the following definitions shall apply:

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,

[6] In line with Article 3 of Joint ESA decision published on 08 November 2024

[7] In line with the CSSF communiqué published on 15 January 2025 "Entry into application of DORA regulation on 17 January 2025".

	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 section 3.1.2. are fulfilled.
2) Client interface	the software layer made available by the cloud computing service provider to the Financial Entity allowing the latter to manage its cloud computing resources.
3) Cloud computing resource	any computing capabilities (e.g. server, storage, network, etc.) provided by a cloud computing service provider.
4) Cloud computing service provider	any firm proposing cloud services within the meaning of the definition provided in section 3.1.2.
5) 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.

3.1.2. Definition of "cloud computing"

23. Cloud computing is a model composed of the following five essential characteristics[8]:

    a. On-demand self-service: A Financial Entity[9] 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 (Financial) Entities using a multi-tenant model[10], with different physical and virtual resources dynamically assigned and reassigned

[8] 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 Network and Information Security (ENISA).

[9] For the sake of clarity, the definition considers the case where the Financial Entity is itself the resource operator.

[10] A physical or logical infrastructure serving several (Financial) Entities through shared cloud computing resources and by means of a standardised model.

according to Financial Entity demand. There is a sense of location independence in that the Financial 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 Financial 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 Financial Entity of the utilised service.

24. Services are considered as cloud computing services within the meaning of this circular if the five essential characteristics defined in point 23 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 a Financial Entity owns on a cloud computing infrastructure without prior and explicit agreement of the Financial Entity and without monitoring mechanism available to the Financial 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 (Financial) Entities of the cloud computing service provider[11]. 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 Financial Entity[12] (e.g. provisioning, configuration or release of cloud computing resources). Thus, the resource operator alone (i.e. either the Financial 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 Financial Entity); or

        ii. within the context of a specific request by the Financial Entity (e.g. provisioning of a cloud computing resource that is missing in the catalogue

[11] In cases of extreme emergency, the Financial Entity should be informed a posteriori.

[12] Indeed, it is an automated system that allows provisioning resources, hence point 24(a) specifying that staff may not have access by default to Financial Entity resources.

proposed by the cloud computing service provider or performing insufficiently).

Sub-chapter 3.2. Cloud officer

25. Furthermore, the CSSF reminds Financial Entities that they shall *ensure and maintain adequate competences within the financial entity in the management and security of the service used* as specified in the RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework[13], Article 11(2)(k)(c). They shall also ensure *a clear allocation of information security roles and responsibilities between the financial entity and the ICT third-party service provider, in accordance with the principle of full responsibility of the financial entity over its ICT third-party service provider* as specified in the same RTS, Article 11(2)(k)(b).

26. In this context the resource operator shall designate among its employees one person, the "cloud officer".

    a. The cloud officer shall be responsible for the use of cloud services and shall guarantee the competences of the staff managing cloud computing resources. The resource operator shall assign the function of "cloud officer" to a qualified person that masters the challenges of an ICT arrangement with a cloud computing infrastructure. The "cloud officer" shall have sufficient competences to take on its function based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider. This "cloud officer" function may be taken up by persons that already cumulate other functions within the ICT department;

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

[13] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

Chapter 4: Date of application

27. This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Commission de Surveillance
du Secteur Financier

Circular CSSF 25/883

as amended by Circular CSSF 26/915

amending Circular CSSF 22/806 on outsourcing arrangements

Circular CSSF 25/883

as amended by Circular CSSF 26/915

amending Circular CSSF 22/806 on outsourcing arrangements

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 Law of 17 December 2010 relating to undertakings for collective investment (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

Luxembourg, 9 April 2025

Ladies and Gentlemen,

As of 17 January 2025, the provisions of the Digital Operational Resilience Act[1] ("DORA") are applicable to the financial entities as defined in DORA and supervised by the CSSF. DORA has introduced harmonised requirements on the use of ICT third-party services, including ICT outsourcing services which were also in the scope of Circular CSSF 22/806 on outsourcing.

Consequently, to avoid duplication of requirements and to provide legal clarity to the market, the CSSF amends Circular CSSF 22/806 on outsourcing. This amendment reflects the CSSF's continued commitment to ensuring the effective management of ICT third-party risks within the financial sector while adhering to evolving European regulatory frameworks.

This circular is to be read in conjunction with Circular CSSF 25/882 on requirements on the use of ICT third-party services for Financial Entities subject to DORA, which complements and provides practical instructions in relation to certain provisions of DORA.

This circular amends Circular CSSF 22/806 by specifying the following:

1. the introduction has been modified to reflect the entry into application of DORA;

2. the definitions of Part I, Chapter 1 have been modified by adding a definition of DORA;

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

3. the scope of application of Circular CSSF 22/806, as described in Part I, Chapter 2 has been modified to consider the entry into application of DORA:

    a. for financial entities as defined in Article 2 of DORA[2] and supervised by the CSSF, for which Circular CSSF 22/806 applied in full for all outsourcing arrangements:

        i. Part I of Circular CSSF 22/806 remains applicable for outsourcing arrangements other than ICT outsourcing;

        ii. Part II of Circular CSSF 22/806, related to ICT outsourcing arrangements, does not apply to them anymore.

    b. for entities falling under Circular CSSF 22/806 but not falling under DORA, and for which Circular CSSF 22/806 applies in full, the latter remains applicable for all outsourcing arrangements in its entirety (Part I and Part II);

    c. for financial entities as defined in Article 2 of DORA and supervised by the CSSF, for which Circular CSSF 22/806 applied in full only when performing ICT outsourcing, Circular CSSF 22/806 no longer applies. Those entities have been removed from the scope;

    d. for management companies authorised only under Article 125-1 of Chapter 16 of the UCITS Law, which consequently are not in the scope of DORA, Circular CSSF 22/806 continues to apply in full when performing ICT outsourcing.

4. The requirement of specific contractual clauses for cloud computing service providers (contract subject to the law of one of the Member States of the EEA and a resilience of the cloud computing services provided in the EEA) have been repealed to align the requirements for the entities under the scope of this circular with the requirements for the entities in the scope of DORA.

The amendments to Circular CSSF 22/806 are shown in "track changes" hereafter.

This circular shall apply with immediate effect.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex Circular CSSF 22/806 as amended by Circular CSSF 25/883

[2] Including third-country branches of financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of DORA, if in the third country where their head office is established, they would qualify as entities listed under Article 2(1)(a) to (t) of DORA.

Commission de Surveillance du Secteur Financier

Circular CSSF Circular CSSF 25/892

as amended by Circular CSSF 26/915

Application of the Joint ESA Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)

Circular CSSF 25/892

as amended by Circular CSSF 26/915

Application of the Joint ESA Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)

To all financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554[1] on digital operational resilience for the financial sector (hereafter "DORA").

To all third-country branches of financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of DORA, if in the third country where their head office is established, they would qualify as entities listed under Article 2(1) (a) to (t) of DORA.

Luxembourg, 27 May 2025

Ladies and Gentlemen,

The purpose of this circular is to inform you that the CSSF, in its capacity as competent authority, applies the Joint Guidelines of the European Supervisory Authorities (ESAs) on the estimation of aggregated annual costs and losses caused by major ICT-related incidents referred to in Article 11(11) of DORA (i.e. JC/GL/2024/34; hereafter the "Guidelines").

This circular is divided into three chapters:

- Chapter 1 defines the scope of application;
- Chapter 2 clarifies the reporting obligation to the CSSF;
- Chapter 3 provides for the entry into force of this circular.

The guidelines are attached as an annex to this circular.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Chapter 1: Scope of application

1. The following entities, other than microenterprises as defined in Article 3(60) of DORA[2], are to be considered as financial entities in the framework of this circular:

   a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements with a derogation and authorised reporting mechanisms with a derogation within the meaning of the Law of 5 April 1993 on the financial sector;
   b) payment institutions, account information service providers and electronic money institutions within the meaning of the Law of 10 November 2009 on payment services;
   c) crypto-asset service providers and issuers of asset-referenced tokens within the meaning of Regulation (EU) 2023/1114;
   d) central securities depositories within the meaning of the Law of 6 June 2018 on central securities depositories;
   e) central counterparties within the meaning of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories;
   f) management companies incorporated under Luxembourg law and subject to Chapter 15 or Article 125-2 of Chapter 16, and Luxembourg branches of investment fund managers subject to Chapter 17, and investment companies which did not designate a management company within the meaning of Article 27 of the Law of 17 December 2010 relating to undertakings for collective investment;
   g) alternative investment fund managers authorised under Chapter 2 and internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the Law of 12 July 2013 on alternative investment fund managers;
   h) institutions for occupational retirement provisions authorised in accordance with Article 2(2) of the Law of 13 July 2005 on institutions for occupational retirement provision in the form of pension savings companies with variable capital (SEPCAVs) and pension savings associations (ASSEPs);
   i) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of Regulation (EU) 2016/1011;
   j) crowdfunding service providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;
   ~~j)~~k) third-country branches of undertakings listed under point 1.a) to j) above and having their head office in a third country that would qualify under Article 2(1) (a) to (t) of DORA.

2. Branches in Luxembourg of the financial entities that are part of a legal entity whose head office is located in a different Member State of the European Union (EU branches) are expected to report their estimations under DORA to the competent authority of that Member State (home Member State) upon its request and are therefore excluded from the scope of this circular.

[2] 'microenterprise' means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million.

Chapter 2: Reporting obligation to the CSSF

3. As required in Article 11(10) of DORA, financial entities shall, upon request, make available to the CSSF an estimation of aggregated annual costs and losses of major ICT-related incidents.

4. The CSSF, in its capacity as competent authority, applies in full the Guidelines and integrates them into its administrative practice and regulatory approach with a view to promoting supervisory convergence in this field at European level.

5. The estimation referred to in paragraph 3 above shall be done in line with the Guidelines and submitted by using the "reporting template for gross costs and losses and financial recoveries in the reference year" as defined in the Annex I of the Guidelines.

Chapter 3: Date of application

6. This circular shall apply as from 31 May 2025.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex Joint Guidelines of the European Supervisory Authorities (ESAs) on the estimation of aggregated annual costs and losses caused by major ICT-related incidents referred to in Article 11(11) of DORA (JC/GL/2024/34).

Commission de Surveillance du Secteur Financier

Circular CSSF 25/893

as amended by Circular CSSF 26/915

on reporting of major ICT-related incidents and significant cyber threats under the Digital Operational Resilience Act (DORA)

Circular CSSF 25/893

as amended by Circular CSSF 26/915

on reporting of major ICT-related incidents and significant cyber threats under the Digital Operational Resilience Act (DORA)

To all financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554[1] on digital operational resilience for the financial sector (hereafter "DORA") and to all Payment Service Providers as referred to in Article 1(37) of the Law of 10 November 2009 on payment services (LPS).

To all third-country branches of financial entities defined in Article 2(1)(a) to (i), (k) to (m), (p), (r) and (s), and within the meaning of Article 2(2) of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (hereafter "DORA"), if in the third country where their head office is established, they would qualify as entities listed under Article 2(1) of Regulation (EU) 2022/2554 (DORA).

Luxembourg, 27 May 2025

Ladies and Gentlemen,

As defined in Articles 18(1), 18(2), 19(1) and 19(2) of DORA, financial entities subject to DORA are required to comply with the obligations for classifying and reporting major ICT-related incidents and, if applicable, significant cyber threats. The specifics regarding classification and reporting are detailed in the following Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS):

- RTS on classification of ICT-related incidents and cyber threats[2] (hereafter "RTS on classification"), and
- RTS and ITS on incident and voluntary cyber threats reporting (hereafter "RTS on incident reporting"[3] and "ITS on incident reporting"[4])

Furthermore, with this circular the CSSF requires Payment Service Providers (PSPs) that are not in the scope of DORA to follow the ICT-related incident and cyber threat classification and reporting procedures under DORA in order to fulfil the reporting requirements stipulated under Article 105-2

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

[2] Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents

[3] Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats

[4] Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat

of the LPS. As a simplification, these PSPs shall follow the DORA requirements for all ICT-related incidents (i.e. including ICT-related incident not related to payment services), so as to avoid a dual reporting scheme.

In this context, this circular also provides the practical modalities according to which financial entities in scope of this circular are required to notify the major ICT-related incidents as well as, if applicable, significant cyber threats to the CSSF.

This circular is divided into four chapters:

- Chapter 1 defines the scope of application;
- Chapter 2 lists the requirements on classification and reporting of incident and cyber threats for PSPs not under DORA;
- Chapter 3 defines the practical modalities for the reporting of major ICT-related incidents and significant cyber threats;
- Chapter 4 provides for the entry into force of this circular.

TABLE OF CONTENTS

Chapter 1: Scope of application

1. The following entities are to be considered as financial entities in the framework of this circular:

   a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements with a derogation and authorised reporting mechanisms with a derogation within the meaning of the Law of 5 April 1993 on the financial sector (LFS);
   b) payment institutions, account information service providers and electronic money institutions within the meaning of the LPS;
   c) crypto asset service providers and issuers of asset-referenced tokens within the meaning of Regulation (EU) 2023/1114;
   d) central securities depositories within the meaning of the Law of 6 June 2018 on central securities depositories;
   e) central counterparties within the meaning of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories;
   f) management companies incorporated under Luxembourg law and subject to Chapter 15 or Article 125-2 of Chapter 16, and Luxembourg branches of investment fund managers subject to Chapter 17, and investment companies which did not designate a management company within the meaning of Article 27 of the Law of 17 December 2010 relating to undertakings for collective investment;
   g) alternative investment fund managers authorised under Chapter 2 and internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the Law of 12 July 2013 on alternative investment fund managers;
   h) institutions for occupational retirement provisions authorised in accordance with Article 2(2) of the Law of 13 July 2005 on institutions for occupational retirement provision in the form of pension savings companies with variable capital (SEPCAVs) and pension savings associations (ASSEPs);
   i) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of Regulation (EU) 2016/1011;
   j) crowdfunding service providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;
   k) Payment Service Providers (PSPs) as referred to in Article 1(37) of the LPS that are not financial entities as defined in point 1 (a) and (b) above, i.e. ~~branches in Luxembourg of PSPs incorporated in a third country, and~~ POST Luxembourg;
   ~~k)~~l) third-country branches of undertakings listed under points 1.a) to j) above and having their head office in a third country that would qualify under Article 2(1) (a) to (t) of DORA.

2. The provisions of Chapter 2 of this circular are only applicable to entities in scope as defined in point (k) above, hereafter collectively referred to as "**PSPs not under DORA**".

3. The provisions of Chapter 3 of this circular are applicable to all financial entities in scope as defined in point 1 (a) to (l~~k~~) above, hereafter collectively referred to as "**Financial Entities**" or individually as "**Financial Entity**", including their branches as specified in the respective laws.

4. Branches in Luxembourg of the Financial Entities that are part of a legal entity whose head office is located in a different Member State of the European Union (EU branches) are expected to report their major ICT-related incidents and significant cyber threats under DORA to the competent authority of that Member State (home Member State) and are therefore excluded from the scope of this circular.

Chapter 2: Requirements on classification and reporting of incident and cyber threats for PSPs not under DORA

5. For the purpose of this circular, the following definitions are derived from the DORA regulation and apply for PSPs not under DORA:

   a) 'network and information system' means:
      (1) an 'electronic communications network': transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;
      (2) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or
      (3) digital data stored, processed, retrieved or transmitted by elements covered under points (1) and (2) for the purposes of their operation, use, protection and maintenance;

   b) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

   c) 'operational or security payment-related incident' means a single event or a series of linked events unplanned by the financial entities, whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity;

   d) 'ICT-related incident' means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity. This includes operational or security payment-related incidents;

   e) 'major operational or security payment-related incident' means an operational or security payment-related incident that has a high adverse impact on the payment-related services provided;

f) 'major ICT-related incident' means an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity. This includes major operational or security payment-related incidents;

g) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

h) 'significant cyber threat' means a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident;

i) 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.

6. PSPs not under DORA are required to classify their ICT-related incidents and their cyber threats according to the criteria and materiality thresholds as defined in Chapters I, II and III of the RTS on classification. Chapters IV and V of the RTS on classification are not applicable to them.

7. PSPs not under DORA are further required to notify the major ICT-related incidents and, if applicable, significant cyber threats, according to the RTS on incident reporting and to the ITS on incident reporting, which apply in full to them.

Chapter 3: Practical modalities for major ICT-related incident notification and significant cyber threats reporting

8. Major ICT-related incident notifications as well as, if applicable, significant cyber threats, shall be submitted via the corresponding form either through the dedicated procedure "DORA Major ICT-related Incident Notification" available on the CSSF eDesk Portal or via the API interface (S3) provided by the CSSF.

9. Financial entities shall notify the CSSF according to the time limits laid down in Article 5 of the RTS on incident reporting. In the exceptional event that a technical impossibility prevents the financial entities from submitting incident notifications using the indicated channel, they shall inform the CSSF via e-mail (ictrisksupervision@cssf.lu), without undue delay and no later than the respective time limits for the submission of the notification or report and shall explain the reasons for the use of the alternative channel.

10. Financial entities shall complete the relevant section(s) of the notification form, depending on the phase they are in. The first section refers to the initial notification as per Article 2 of the RTS on incident reporting, the second section refers to the intermediate report as per Article 3 of the RTS on incident reporting and the third section refers to the final report as per Article 4 of the RTS on incident reporting. The notification form contains the data fields laid down in Annexes II and IV of the ITS on incident reporting.

11. Article 7 of the ITS on incident reporting indicates that aggregated reporting is only possible if competent authorities have explicitly given the permission. In this regard, the CSSF informs financial entities that, after having carefully evaluated all of the conditions from points (a) to (d) of Article 7(1) as well as Article 7(2) of the ITS on incident reporting, no aggregated report is permitted when it comes to major ICT-related incident notifications.

12. Financial entities that have outsourced the reporting obligations remain fully responsible for the fulfilment of incident reporting requirements within the applicable timeline and for the whole content of the notification forms. As specified in Article 6 of the ITS on incident reporting, financial entities shall inform the CSSF as soon as possible of outsourcing of reporting obligations and at the latest prior to the first notification. In this regard, the following details must be provided to the CSSF (email address: ictrisksupervision@cssf.lu):

    a) Name, contact details and an identification code of the third party that will submit the notifications on behalf of the financial entity;
    b) Name, contact details and the related function of the persons at the third party to whom the related incident notification role will be assigned in the CSSF digital solution.

Chapter 4: Date of application

13. For entities listed under points 1(a) to (j) and (l):

    a) This circular shall apply with immediate effect and renders Circular CSSF 24/847 on ICT-related incident reporting framework no longer applicable to them;

    b) Circular CSSF 21/787 on application of the EBA Guidelines (EBA/GL/2021/03) on major incident reporting under PSD2 is no longer applicable to them.

14. For entities listed under point 1(k):

    a) This circular shall apply six months after its publication date;

    b) During the transition period, the classification criteria as well as the notification reporting modalities as required by Circulars CSSF 24/847 on ICT-related incident reporting framework and CSSF 21/787 on application of the EBA Guidelines (EBA/GL/2021/03) on major incident reporting under PSD2 remain applicable to them.

15. Six months after the publication date of this circular, Circular CSSF 21/787 on application of the EBA Guidelines (EBA/GL/2021/03) on major incident reporting under PSD2 will be repealed.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General