Commission de Surveillance
du Secteur Financier

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 25/882

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 (hereafter "DORA") [1].

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 in the scope of this circular:

   a) credit institutions, investment firms, market operators operating a trading venue and approved publication arrangements (APAs) with a derogation and authorised reporting mechanisms (ARMs) 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 (CSD Law);

   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 (AIFM Law);

   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.

2. The provisions of this circular are applicable to all financial entities in scope as defined in point 1(a) to (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 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.

[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.

[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.

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.

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.

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

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, 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

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

	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 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.

[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.

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 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,

[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.

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.

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

[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