CSSF aligns outsourcing rules with DORA framework

By Vincent WELLENS, Avocat à la Cour & Ottavio COVOLO, Avocat à la Cour, NautaDutilh Avocats Luxembourg S.à r.l.

On 9 April 2025, the CSSF has published amendments to several circulars to bring them in line with the Digital Operational Resilience Act ("DORA") just ahead of the first deadlines of reporting by in-scope entities.

The CSSF first announced changes to CSSF Circular 20/750, which sets out rules concerning entities' ICT security management. This circular applied to all credit institutions, professionals of the financial sector ("**PFS**") as well as payment and e-money institutions ("**PSPs**" and "**EMIs**") and - content-wise - was mainly a formal adoption of the EBA Guidelines on ICT and security risk management EBA/GL/2019/04. The EBA amended such guidelines on 11 February 2025 removing all but section 3.8 regarding payment and e-money institutions to avoid unnecessary overlaps with DORA.

As a reminder, these EBA guidelines, applicable without prejudice to the other EBA guidelines on outsourcing, required financial entities to adopt a risk-based approach to ICT risk management, with requirements which remain general compared to the specific provisions of DORA. For instance, paragraph 9 of the

EBA guidelines set out a general monitoring requirement for third parties (to be read with the broader monitoring requirements of ICT risks of the institution) but does not go as far as the like requirements under DORA.

The CSSF implemented this amendment to the EBA through changes to Circular 20/750, which will mean:
- for **credit institutions and DORA in-scope entities**, only the requirements under DORA should be followed.
- for **PSPs and EMIs**, the CSSF has decided to moving the PSP and EMI-relevant provisions regarding their ICT assessment into a standalone Circular 25/880. PSPs

and EMIs should therefore update their internal ICT policy references to the 20/750 circular with this new one.
- for **other entities falling outside the scope of DORA** - such as support PSFs – the circular CSSF 20/750 will continue to apply as usual.

The other main development was the update to CSSF Circular 22/806 on outsourcing arrangements, transposing the 2019 EBA Guidelines on outsourcing arrangements EBA/GL/2019/02 along with gold-plating language extending the scope of the obligations therein on a few points (and also extending the personal scope to other actors that are not concerned by the EBA guidelines).

Unlike the EBA Guidelines on ICT and security risk management, the EBA Guidelines on outsourcing arrangements have yet to be updated to be aligned with DORA, leading to in-scope entities performing gap analysis regarding the two overlapping sets of requirements, with sometimes at first sight minor but critical differences.

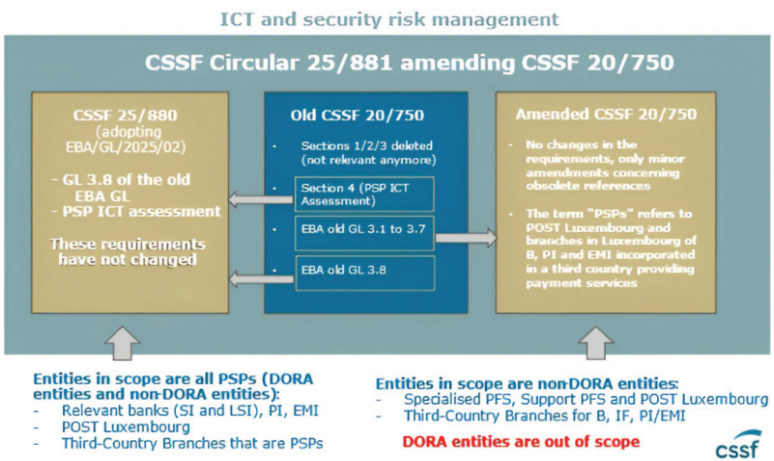
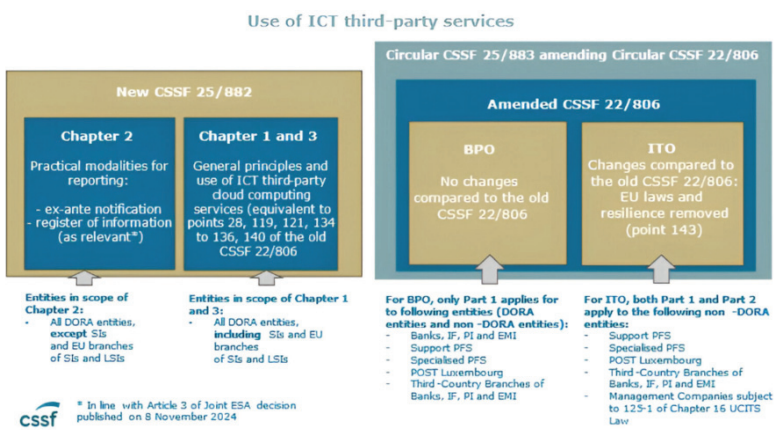
For instance, CSSF Circular 22/806 requires a list of obligatory points to be integrated in outsourcing agreements, whether the outsourcing is critical or not (even when the 2019 EBA outsourcing guidelines made such a distinction). In comparison, DORA works on the basis of a list of clauses for all ICT agreements and one only limited to critical ICT services. Further, there are slight differences in wording that can make a major difference in contract negotiations.

For example, paragraph 101(a) of CSSF Circular 22/806 required a right of termination by the in-scope entity in case of a "*breach of applicable law, regulations or contractual provisions* ", whereas article 28.7.a of DORA refers instead to a "*significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms*", which is a wording more in favour of the ICT service provider.

To mitigate such differences, albeit without any finalised update yet from the EBA, the CSSF has proceeded to the following updates:
- for **non-DORA entities** (including management companies of SIFs, SICARs, limited partnerships or SOPARFIs which do not qualify as AIFs), the amended the Circular 22/806 will continue to be fully applicable to all outsourcings, including both business process (outside the scope of DORA) and ICT outsourcing. The provisions specific to cloud infrastructure-based ICT outsourcing also remain in place.

However, paragraph 143 regarding the principal requirement to have an EU Member State law as law applicable to the agreement with the cloud computing service provider has been repealed, with the CSSF citing the absence of such requirement under DORA and the interest in aligning this requirement between DORA and non-DORA entities as the reason for such removal.
- for **DORA entities**, the amended CSSF Circular 22/806 sections relating to business process outsourcing will remain applicable (including the notification of critical and important functions regarding such processing).

ICT outsourcings will exclusively be subject to a new Circular 25/882 incorporating the requirements to keep daily backup of accounting positions, prior notification of critical and important ICT functions outsourcing (under the same timelines as under Circular 22/806), and some of the cloud computing provisions of Circular 22/806. The new circular notably clarifies that when the so-called cloud "*resource operation*" is carried by a service provider in Luxembourg, it must in principle be authorised by the CSSF in accordance with Article 29-3 of the 1991 Law on the Financial Sector (a so-called IT Support Financial Sector Professional) to provide such service.[1]

The CSSF Circular 25/882 also provides a confirmation that the register of contractual arrangements under DORA shall be submitted annually between 28 February and 31 March of the next year (with 2025 having an exceptional deadline between 1 April 2025 and 15 April 2025 in line with the CSSF January 2025 press release on the matter).

1) Or, if not, the service provider must be 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.