Commission de Surveillance
du Secteur Financier

# Circular CSSF 25/880

## on relationship management of payment service users and PSP ICT assessment

# Circular CSSF 25/880

## on relationship management of payment service users and PSP ICT assessment

To all Payment Service Providers as referred to in Article 1(37) 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[1] ("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")[2] and Article 95(3) of Directive (EU) 2015/2366 (Payment Services Directive 2, "PSD2") [3]. 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[4].

This circular transposes the new EBA Guidelines, which will be applicable for all PSPs, including branches in Luxembourg of PSPs incorporated in a third country, and POST Luxembourg, within the scope of the Law of 10 November 2009 on payment services (LPS) and supervised by the CSSF. Furthermore, 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 is integrated into 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 (DORA)

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

[3] 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) (PSD2)

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

This circular is divided into three chapters:

- Chapter 1 implements the EBA Guidelines EBA/GL/2025/02 amending Guidelines EBA/GL/2019/04 on ICT and security risk management. The CSSF considers that the content of these Guidelines reflects its expectations as regards the relationship management of the payment service user and has, via this circular, integrated them into its administrative practice and regulatory approach;
- Chapter 2 lists the requirements on PSP ICT assessment, according to which PSPs are asked to provide the CSSF with an updated and comprehensive PSP ICT assessment. This has not changed with the entry into application of DORA and PSPs shall continue to fulfil the requirements stated under points 8 to 11 of this circular;
- Chapter3 provides for the entry into force of this circular.

**TABLE OF CONTENTS**

## Chapter 1. Relationship management of the payment service users (PSUs)[5]

1. PSPs should establish and implement processes to enhance PSUs' awareness of the security risks linked to the payment services by providing PSUs with assistance and guidance.
2. The assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the PSU.
3. Where product functionality permits, PSPs should allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU.
4. Where, in accordance with Article 82(1) of the LPS, a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the PSP should provide the payer with the option to adjust these limits up to the maximum agreed limit.
5. PSPs should provide PSUs with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.
6. PSPs should keep PSUs informed about updates in security procedures that affect PSUs regarding the provision of payment services.
7. PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. PSUs should be appropriately informed about how such assistance can be obtained.

## Chapter 2. PSP ICT assessment

8. In accordance with Article 105-1(2) of the LPS, PSPs are required to provide the CSSF with an updated and comprehensive risk assessment related to payment services (hereafter "PSP ICT Assessment"). The CSSF has developed a standardised form for the PSP ICT Assessment to be used by all PSPs. The objective of this standardised PSP ICT Assessment form is to give guidance to the PSPs on the CSSF's expectations on the information to be provided via the PSP ICT Assessment, and hence achieve a certain level of harmonisation and comparability among the PSPs' ICT Assessments.
9. Concerning the scope of the PSP ICT Assessment, the following is to be highlighted:
   a) Institutions whose business model does not include the provision of payment services (as defined in article 1(38) of the LPS), do not have to provide the PSP ICT Assessment. As soon as the business model of an institution includes the provision of payment services, it shall submit a PSP ICT Assessment to the CSSF for that calendar year.
   b) EEA Branches established in Luxembourg which offer payment services do not have to provide the CSSF with a PSP ICT Assessment. On the other hand, Luxembourg-based PSPs with branches in other EEA countries which provide payment services, have to include those branches in their PSP ICT Assessment. In the event the ICT and security

[5] As defined in Article 1(46) of the LPS

risk assessment for these branches deviates from that of the PSP, it should be made clear in the PSP ICT Assessment[6].

10. All PSPs must submit the duly completed PSP ICT Assessment form on an annual basis to the CSSF **no later than 31 March each year and covering the previous calendar year**.

11. The PSP ICT Assessment form is published in the CSSF's eDesk portal which is available at https://edesk.apps.cssf.lu/.

    The PSP ICT Assessment shall be validated by the Management body of the PSP, i.e. at least by the member of the Management body responsible for the ICT function. This validation shall be specified in the respective section of the PSP ICT Assessment.

    The duly completed and validated PSP ICT Assessment shall be submitted annually by a member of the management body to the CSSF exclusively via the CSSF's eDesk portal.

## Chapter 3. Date of application

12. This circular shall apply with immediate effect.

**Claude WAMPACH**
Director

**Marco ZWICK**
Director

**Jean-Pierre FABER**
Director

**Françoise KAUTHEN**
Director

**Claude MARX**
Director General

[6] See EBA Q&A ID number 2018_4176