Table of Contents

Question ID: 2018_4231

Status
Final Q&A

Legal act
Directive 2015/2366/EU (PSD2)

Topic
Security measures for operational and security risks

Article
95

Paragraph
2

Subparagraph

COM Delegated or Implementing Acts/RTS/ITS/GLs
EBA/GL/2017/17 - Guidelines on security measures for operational and security risks under PSD2

Article/Paragraph
3 / 4

Date of submission
06/09/2018 10:45

Published as Final Q&A
19/07/2019 13:08

Type of submitter
Credit institution

Subject matter
Responsibility for comprehensive assessment according to Article 95(2) PSD2

Question

It is not clear, whether comprehensive assessment of the operational and security risks relating to the payment services has to be carried out by the payment service providers (PSP), or it can be delegated / outsourced to a third entity (e.g. external audit firm). In case this is a responsibility of the PSP, it is not clear, whether it has to be carried by the independent internal audit department, or it has to be carried out by the department responsible for the risk function in the PSP.

Background on the question

From the PSD2 Directive is not clear whether PSP has to carry out "Comprehensive assessment of the operational and security risks relating to the payment services" by itself, or this can be delegated to third party (audit firm, independent valuator / consultancy firm).

In PSD2, there is only responsibility for providing mentioned (and we do not argue with that) - PSP will be responsible for providing this to authorities, but it is not clear, whether the performance of this assessment / report can be outsourced to relevant third party.

We do not have internal capacities to carry out "Comprehensive assessment of the operational and security risks relating to the payment services", and we are seeking for possibilities to outsource this, but it is not clear, whether we can.

EBA answer

The EBA Guidelines on security measures for operational and security risks of payments services under PSD2 (EBA/GL/2017/17) do not list the operational functions that can be outsourced. Instead, they state the following principles to follow when outsourcing: (i) the need to ensure the effectiveness of the security measures set for the referred outsourced operational functions and (ii) the need to ensure that measures and performance targets are built into contracts and service-level agreements with the providers to whom they have outsourced such functions (Guidelines 2.7 and 2.8 of these EBA Guidelines). Furthermore, payment service providers (PSPs) should have regard to the general principles of outsourcing as specified under PSD2 and/or CRD IV (depending on the type of license), in particular, that PSPs retain full responsibility when outsourcing and therefore should comply with all the regulatory requirements.

Accordingly, the risk assessment referred to in Article 95 of PSD2 could be outsourced, provided such outsourcing complies with the afore-mentioned principles and provisions in PSD2 and in the Guidelines.

Finally, it should be noted that outsourcing of the risk assessment should also be done in accordance with

the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02). The Guidelines on outsourcing arrangements are addressed to all PSPs and are in line and should be read in conjunction with the requirements of PSD2 and the Guidelines on security measures for operational and security risks of payments services.

Link
EBA website link