Presentation of the PSP ICT Assessment form

The presentation of the PSP ICT Assessment form as shown here in a PDF version varies from the version to be submitted via the eDesk portal of the CSSF

The present document is only for information purposes.

The PSP ICT Assessment shall be duly completed and validated by using the form published in the CSSF's eDesk portal and submitted to the CSSF exclusively via that eDesk portal.

PSP ICT Assessment - Context and instructions

CONTEXT

Legal and regulatory references

Pursuant to article 105-1(2) of the amended law of 10 November 2009 on payment services ("**LPS**"), payment service providers ("**PSP**"; as defined by article 1(37) of the LPS) shall provide to the CSSF, at least on an annual basis, an **updated and comprehensive assessment** of the operational and security risks relating to the **payment services** they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

Pursuant to point 4. "Additional requirements for PSPs" of the amended circular CSSF 20/750 on the requirements regarding information and communication technology ("**ICT**") and security risk management ("**Circular**"), PSPs are required to provide the CSSF with an **updated and comprehensive risk assessment** ("**PSP ICT Assessment**"), as provided in point 24. of of the part 3.3.5. "Reporting" of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) ("**ICT Guidelines**").

Objective

The objective of the present 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' PSP ICT Assessments.

PSPs are required to complete and submit the present form at least on an annual basis according to the instructions indicated under point 4. "Additional requirements for PSPs" of the Circular.

Scope

Pursuant to Article 105-1(2) of the LPS and point 4. "Additional requirements for PSPs" of the Circular, the PSP ICT Assessment shall cover the **ICT and security risks** (as defined under point 10. of the part "Subject matter, scope and definitions" of the ICT Guidelines) related to **payment services** (as defined in article 1(38) of the LPS) provided by the PSPs.

Institutions, whose **business model does not include the provision of payment services**, 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 to the CSSF for that calendar year a PSP ICT Assessment according to the instructions indicated under point 4 "Additional requirements for PSPs" of the Circular.

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 which have established 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 risk assessment for these branches deviates from that of the PSP, it should be made clear in the PSP ICT Assessment (see EBA Q&A ID number 2018_4176).

INSTRUCTIONS

The present form contains the following parts: Context-Instructions, General Information, Functions-Processes-Assets, ICT & Security Risks (1), ICT & Security Risks (2), Tests on Security Measures, Conclusions.

All fields are mandatory and are required to be filled in before submission of the PSP ICT Assessment to the CSSF (except for the fields indicated as optional).

Concerning the parts "ICT & Security Risks (1)" and "ICT & Security Risks (2)", every ICT and security risk shall, not only be classified based on the risk methodology of the institution, but also be categorised pursuant to one of the **risk categories**. These risk categories are based on the respective sections of the ICT Guidelines (except for the category "manual intervention").

RISK CATEGORIES

Risk categories	Examples
Governance and strategy	Inadequate IT organisation
	Inadequate IT strategy
	Inadequate allocated IT budget
	Inadequate IT staffing
	Inadequate outsourcing governance
ICT and security risk management framework	Inadequate ICT and security risk management framework
	Inadequate identification of functions, processes and assets
	Inadequate reporting to the management body
	Inadequate internal IT audit
Information security	Inadequate information security policy
	Inadequate logical ICT security
	Inadequate physical ICT security
	Inadequate security monitoring
	Lack of information security reviews
	Inadequate protection of communication channels used for payments (data in transit)
	Inadequately secured ICT systems used for payments
	Inadequate encryption of data at rest
	Inadequate vulnerability management
	Inadequate patch management
	Inadequate security of third party or another Group entity
	Inadequate information security training and awareness (Unsafe behaviour of users and PSPs)
ICT operations management	Inadequate inventory of ICT assets
	Inadequate performance and capacity management
	Inadequate logging and monitoring procedures
	Inadequate incident and problem management
	Inadequate backup and restore procedures
ICT project and change management	Inadequate ICT project management
	Inadequate ICT systems acquisition and development management
	Inadequate ICT change management
Business continuity management	Inadequate business impact analysis performed
	Inadequate ICT continuity and disaster recovery planning
	Inadequate resilience of third party or another Group entity services
	No regular tests performed
	ICT system failures
	Disruptive and destructive cyber attack
Manual intervention	Erroneous manual interventions relating to the management, execution, monitoring, etc., of payment services

PSP ICT Assessment - General Information

Calendar year concerned *(yyyy)*	

PSP

Name of the PSP	
Public register number *(e.g. B00000001)*	

Contact person

Name	
Function / position	
Phone number	
E-mail address	

Validation of the ICT Assessment

1. Name of the member of the management body	
Date of validation *(dd/mm/yyyy)*	
2. Name of the member of the management body *(optional)*	
Date of validation *(dd/mm/yyyy)*	
3. …	

Comments *(optional)*

PSP ICT Assessment - Business functions, supporting processes and information assets

Please, provide a summary of the most critical business functions, supporting processes and information assets identified related to payment services provided, and describe their interdependencies related to ICT and security risks, according to §§ 15, 16 and 17 of the ICT Guidelines:

Comments *(optional)*

PSP ICT Assessment - ICT and security risks related to business functions, supporting processes and information assets (1)

Please, provide the number of risks identified and classified per risk level based on your methodology (for example: critical, high, medium, low) for the inherent risk and residual risk, as well as per risk category:

Inherent risk *(ranked highest to lowest)*

Risk level	Number of risks
Total :	0

Residual risk *(ranked highest to lowest)*

Risk level	Number of risks
Total :	0

Risk category

Risk category	Number of risks
Governance and strategy	
ICT and security risk management framework	
Information security	
ICT operations management	
ICT project and change management	
Business continuity management	
Manual intervention	
Total :	0

Comments *(optional)*

PSP ICT Assessment - ICT and security risks related to business functions, supporting processes and information assets (2)

Please, list in the table here below the 10 highest rated ICT and security risks based on the inherent risk as determined by your methodology provided in the part "ICT & Security Risks (1)". The description of these risks and their mitigation measures need to be sufficiently granular. Only ICT and security risks (as defined by the ICT Guidelines) relating to payment services shall be listed here below.

			INHERENT RISK			MITIGATION MEASURES		RESIDUAL RISK	
#	Detailed description of the 10 highest rated ICT & security RISKS identified *(ranked highest to lowest)*	Risk category	Likelihood of the risk materialising	Potential impact (on the PSP (e.g. financial, reputational, business, regulatory, ...) and its customers)	Inherent risk level	Description of mitigation measures currently in place	Evaluation on the adequacy of the mitigation measures in place	Residual risk level	Comments (*optional*)
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

Comments *(optional)*

PSP ICT Assessment - Tests on security measures of critical ICT systems and audits

Please confirm, according to § 44 of the ICT Guidelines, that the tests of the security measures for all critical ICT systems were performed during the calendar year and that these tests are part of the present PSP ICT Assessment. Otherwise, please explain.

☐ We confirm that these tests were performed, and provide here below a summary of the results:

☐ We do not confirm that these tests were performed, and provide here below the reason:

cssf
Commission de Surveillance du Secteur Financier

PSP ICT Assessment - Conclusions

Conclusion on the adequacy of the management of the ICT and security risks, in particular on the materiality of residual risks relating to ICT and security risks (considering a.o. the PSP's risk appetite) and on the mitigation measures foreseen to reduce these residual risks: