Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

Guidance on the PSD2 Operational and Security Risk Assessment Return

March 2020

Table of Contents

1. Introduction

Directive 2015/2366/EU on payment services (or "PSD2") was transposed into Irish law, with effect from 13 January 2018, by the European Union (Payment Services) Regulations 2018 (S.I. No. 6 of 2018, hereafter referred to as the Payment Services Regulations 2018). The Payment Services Regulations 2018 place a number of reporting requirements on payment service providers ("PSPs").

Regulation 118 of the Payment Services Regulations 2018 imposes a number of requirements on PSPs with respect to the management of operational and security risks:

> *118. (1) a payment service provider shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services that it provides.*
>
> *118. (2) As part of the framework referred to in paragraph (1), a payment service provider shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.*
>
> *118. (3) A payment service provider shall provide to the Bank on an annual basis, or at shorter intervals as determined by the Bank, an updated and comprehensive assessment of:*
>
> *(a) the operational and security risks relating to the payment services provided by the payment service provider, and*
>
> *(b) the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.*

In order to facilitate PSPs in providing the assessment referenced in Regulation 118(3), the Central Bank has developed the 'Operational and Security Risk Assessment' return reporting template. PSPs will be required to complete and submit this template via the Online Reporting System ("ONR") on an annual basis. The Central Bank retains the power to require these reports at shorter intervals on a sectoral, or a firm specific, basis.

The purpose of this document is to provide high-level guidance to PSPs for completion and submission of this return to the Central Bank.

The operational and security risk assessment should refer to the EBA Guidelines on ICT and security risk management. These include:

- high level description of business functions, processes and information assets supporting payment services provided with a focus on the most critical;
- a summary risk assessment of functions, processes and assets against most significant threats and vulnerabilities;
- a summary description of security measures to mitigate security and operational risks identified as a result of the above assessment; and
- conclusions of the results of the risk assessment and summary of actions required as a result of this assessment.

The assessment of the adequacy of mitigation measures and control mechanisms should refer to the EBA Guidelines on security measures for operational and security risks. These include:

- a summary description of methodology used to assess effectiveness and adequacy of mitigation measures and control mechanisms;
- a summary assessment of the adequacy and effectiveness of mitigation measures and control mechanisms; and
- conclusions on any deficiencies identified as a result of the assessment and proposed corrective actions.

This return also includes a section for PSPs to provide information on their top 5 ranked operational and security risks relating to the payment services that they provide.

Please note that a separate user manual, giving more technical details on navigation, sign-off, submission, etc. of the return is available for users in the ONR.

Further information on PSD2 and the reporting requirements that PSD2 places on PSPs, including a link to frequently asked questions, can be found on the Central Bank website at the following link:
https://www.centralbank.ie/regulation/psd2-overview/faq

2. Guidance on completing the "Overview and PSP Details" tab

'PSP Details' Section

This section requires the PSP to enter the following basic details; note that these fields are mandatory and must be completed before submission of the return on the ONR:

- Name of the PSP submitting the assessment
- PSP Reference Number / Institution Code
- PSP Contact Details - Name
- PSP Contact Details – Contact number or email

Additional Questions

Below the PSP Details section on this tab, there are a further 2 mandatory entries required:

- *Please confirm the information submitted in this assessment of operational and security risks (in relation to payment services you provide) is accurate and complete. (Confirm / do not confirm)*

  For this question, indicate in the text box provided that you either 'Confirm' or 'Do not confirm' the accuracy and completeness of the information provided in the template.

- *Date the last assessment of operational and security risks (in relation to payment services you provide) was completed.*

  For this question, enter the relevant date of the last assessment submitted to the Central Bank in the text box provided.

3. Guidance on completing the "Assessment" tab

This section requires the PSP to enter the following assessments; note that these fields are mandatory and must be completed before submission of the return on the ONR:

- *Provide a summary assessment of the operational and security risks related to the payment services you provide.*

  For this question, indicate in the text box provided, a summary assessment of the operational and security risks related to payment services provided by the PSPs. This is to be detailed enough to allow for supervisory review but be completed in no more than 3000 words.

- *Provide a summary assessment of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.*

  For this question, indicate in the text box provided, a summary assessment that should refer to the requirements contained in the EBA Guidelines for operational and security risks of payment services:

  - summary description of methodology used to assess effectiveness and adequacy of mitigation measures and control mechanisms;
  - summary assessment of the adequacy and effectiveness of mitigation measures and control mechanisms.

  Note: Where an action plan or programme to improve the risk rating is referenced, target completion dates are to be provided.

  The answers to these questions are to be detailed enough to allow for supervisory review but should be no more than 3000 words.

- *Additional information*

  Please provide any additional pertinent information relevant to the question.

4. Guidance on completing the "Top 5 Risks" tab

This section requires the PSP to enter the top 5 operational and security risks related to payment services that it provides; note that these fields are mandatory and must be completed before submission of the return on the ONR. Please note that the scoring applied to the "Risk Rating" & "Control Rating" cells should be taken from the PSP's internal rating system.

Overview section

- *Identify the operational and security risks in relation to the payment services the PSP provides (what events might occur that will have a negative impact?)*

For this question, enter the relevant data in the text box provided.

- *Risk description*

For this question, enter a brief description of the risk in the text box provided.

- *Business line/unit*

For this question, enter the business line/unit impacted by the risk. This should reflect whether multiple business units/lines are impacted.

- *Category*

For this question, enter the category of risk in the text box provided i.e. people, system, etc.

'Inherent Risk' section

- *Likelihood: Broadly assess the likelihood of the risk materialising ('coming true')?*
- *Potential impact: Identify the potential impact if the issue/risk were to materialise.*

For these questions, enter a description of the inherent or pre-control risk level in the text boxes provided.

- *Risk Score: Determine the appropriate level of risk related to this issue/risk?*

For this question, enter the internal risk score of the inherent or pre-control risk level in the cell provided.

'Controls assessment' section

- *Existing control: What mitigation measures and control mechanisms are currently in place?*

For this question, enter a description of what mitigation and controls are in place as well as the appropriateness of the controls employed in the text box provided.

- *Control rating: Determine the appropriate controls rating related to this issue/risk.*

For this question, enter the internal risk score of controls in the cell provided.

'Residual Risk' section

 Risk rating: Given the controls listed in column I, what is the subsequent risk rating?

For this question, enter a rating for the residual or post-control risk level in the text boxes provided.

Additional Section

- *Name of person who has responsibility for managing this risk.*

  Please provide the name of the owner of this risk in the text box.

- *Has this risk/issue occurred previously?*

  Please provide the number of instances, brief description of same and whether the instances occurred pre or post controls in the text box.

- *Brief description of the internal risk rating system*

  Please provide a brief description of the internal rate system used for risk scores.

- *Additional Comments*

  Please provide any other information relevant to this risk.

5. Guidance on completing the "Article 17" tab

This section applies to PSPs that are availing of the exemption from applying strong customer authentication for secure corporate payment processes and protocols. This exemption is set out in Article 17 of the Commission Delegated Regulation (EU) 2018/389 with regard to strong customer authentication and common and secure open standards of communication (the RTS).

Initial Question

- *Is the Firm availing of the exemption available under Article 17 of the RTS?*

This is a compulsory question, with a Yes/No dropdown menu. If Yes, firms will be required to complete all questions 1 to 7.

- *Question 1 - Has the Firm previously advised the Central Bank of its use of the Article 17 exemption?*

This question is in the form of a Yes/No dropdown menu also.

- *Question 2 - Confirmation regarding the security of the processes/protocols.*

This is a free text response. Firms should provide the relevant confirmation.

- *Question 3 - Details of processes/protocols*

This is a free text response. Firms should provide a high level summary of the processes/protocols to which the exemption applies.

- *Question 4 - Details of the transaction monitoring mechanism in place*

This is a free text response. Firms should provide a high level summary of the transaction monitoring in place to ensure that their protocols provide at least equivalent levels of security to those provided for by Directive 2015/2366.

- *Question 5 - Secure communication mechanism*

This is a free text response. Firms should provide a high level summary of their secure communication mechanism.

- *Question 6 - Authentication Mechanism*

This is a free text response. Firms should provide a high level summary of the authentication mechanisms in place to guarantee at least equivalent levels of security to those provided for under the RTS.

- *Question 7 - Fraud rates*

  This is a free text response. Firms should provide details of the fraud rates for their exempted processes or protocols, in addition to the fraud rates for their non-exempt business (if applicable).

6. Guidance on inbuilt validations

The template for reporting under Regulation 118(3) of the Payment Services Regulations 2018 has been created in a manner to allow for standardised reporting across PSPs and facilitates consistency across submissions. The template has been locked with only the relevant cells left unlocked for input, PSP's should not alter, delete or add cells/tabs in this template and should review the validation tab to ensure no validation errors remain before submitting the template via ONR.

All fields referenced as mandatory above are required to be filled in before submission or the report will not be accepted by the Central Bank.

Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem