Chapter 16

Reporting requirements

Notes on completing REP018 Operational and Security Risk form

Operational and security risk form

These notes contain *guidance* for *payment service providers* that are required to complete the operational and security risk form in accordance with regulation 98(2) of the *Payment Services Regulations* and ■ SUP 16.13.13D. The *guidance* relates to the assessments that must be attached to the form in accordance with ■ SUP 16.13.13D(2).

The *payment service provider* must attach to the form the latest:

•assessment of the operational and security risks related to the *payment services* the *firm* provides; and

•assessment of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

The operational and security risk assessment should include all the requirements contained in the *EBA* Guidelines for operational and security risks of payment services as issued at 12 December 2017. These include:

•a list of business functions, processes and information assets supporting payment services provided and classified by their criticality;

•a risk assessment of functions, processes and assets against all known threats and vulnerabilities;

•a 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.

Payment service providers intending to make use of the exemption in article 17 of the *SCA RTS* must include:

•a description of the *payment services* that the *payment service provider* intends to provide in reliance on this exemption; and

•an explanation of how the *payment service provider's* processes and protocols achieve at least equivalent levels of security to those provided for by the *Payment Services Directive*.

The assessment of the adequacy of mitigation measures and control mechanisms should include all the requirements contained in the *EBA* Guidelines for operational and security risks of payment services as issued at 12 December 2017. These include:

•a summary description of methodology used to assess effectiveness and adequacy of mitigation measures and control mechanisms;

•an 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.

[**Note:** see https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2]