Boulevard de Berlaimont 14 – BE-1000 Brussels
Phone +32 2 221 48 66
Company number: 0203.201.340
RPM (Trade Register) Brussels
www.nbb.be

BanqueNationaleBank
DE BELGIQUE VAN BELGIË
Eurosystem

Circular

Brussels, 23 November 2021

Reference: NBB_2021_26

Contact person:
Thomas Plomteux
Phone +32 2 221 21 97
thomas.plomteux@nbb.be

Reporting on operational and security risks of payment services to be submitted by payment institutions and electronic money institutions

Scope

Payment institutions governed by Belgian law, registered payment institutions governed by Belgian law providing account aggregation services, limited payment institutions governed by Belgian law, electronic money institutions governed by Belgian law, limited electronic money institutions governed by Belgian law

Summary/Objectives

This circular establishes how payment institutions and electronic money institutions should comply with the reporting obligation imposed by Article 50, § 2 of the Law of 11 March 2018[1]. This circular applies from 1 January 2022 and replaces circular NBB_2020_24, which ceases to apply from that date.

1 The Law of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the activity of payment service provider and the activity of issuing electronic money, and access to payment systems, Belgian Official Gazette of 26 March 2018 (hereinafter referred to as "the Law of 11 March 2018").

Dear Sir,
Dear Madam,

Through this circular, the National Bank of Belgium (hereinafter referred to as "the Bank") aims to clarify the reporting obligation imposed by Article 50, § 2 of the Law of 11 March 2018.

Article 50, § 2 of the Law of 11 March 2018 requires institutions to submit a reporting to the supervisory authority consisting of an updated and comprehensive assessment of the operational and security risks relating to the payment services provided by the institution and of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

With this circular, the Bank wishes to clarify its expectations regarding the report to be submitted annually by the payment institutions governed by Belgian law, the registered payment institutions governed by Belgian law providing account information services, the limited payment institutions governed by Belgian law, the electronic money institutions governed by Belgian law and the limited electronic money institutions governed by Belgian law.

These institutions should submit a detailed and reasoned assessment of the operational and security risks of both the payment services already offered and the payment services expected to be offered within the next year. This means that:

1. the assessment should include the following information for each identified risk:

   - a description of the risk identified, including the implications for the institution and its customers if the risk were to materialise;
   - the inherent risk levels, with an estimation of their probability and their impact on the institution;
   - existing mitigating controls for the risk identified, including a description of their effect on the institution's risk level;
   - the level of residual risk remaining after the implementation of risk mitigation measures;
   - any outstanding actions identified to improve the efficiency of the controls, as well as the planning of their implementation.

2. institutions should provide an assessment of their compliance with the EBA Guidelines on ICT and security risk management, which have been implemented through circular NBB_2020_23[2]. This assessment should include a description of the provisions of these Guidelines which the institution does not comply with, as well as an evaluation of the impact of this non-compliance on the institution's risk level.
3. institutions should also specify any developments that have occurred since the previous submission of the report (or since the authorisation was granted by the Bank).

2 The EBA Guidelines to which this circular refers clarify that the operational risks for payment services refer predominantly to ICT and security risks because of the electronic nature of payment services.

In order to ensure a sufficiently high quality of this reporting and to help institutions as much as possible to fulfil their reporting obligation, the Bank will annually make standardised IT risk questionnaires and practical instructions available to the institutions falling under the scope of application of this circular. These questionnaires will more specifically focus on the inherent exposure of these institutions to a number of ICT risk categories[3] and on the corresponding mitigation measures and controls in a number of ICT risk control areas[4]. Moreover, in the light of the principle of proportionality, these questionnaires may differ from institution to institution, for example depending on the size and internal organisation of the institution concerned or on the nature, scale, complexity and riskiness of the services and products that it provides or intends to provide.

Institutions are expected to complete these questionnaires annually in a sufficiently comprehensive and critical manner. In that case, and if the institution responds adequately to any requests for additional information and/or documentation, the Bank will consider the completion of this questionnaire sufficient to comply with the statutory reporting requirement.

This circular applies from 1 January 2022.

A copy of this circular will be sent to your institution's accredited statutory auditor(s).

Yours faithfully,

p.p. Pierre Wunsch
Governor

Steven Vanackere
Vice-governor

3 The following are some of the categories that may be concerned: ICT availability and continuity risk, ICT security risk, ICT change risk, ICT data integrity risk and ICT outsourcing risk.

4 The following are some of the areas that may be concerned: ICT governance, ICT organisation and ICT outsourcing, ICT risk management, ICT security management, management of ICT operations, software acquisition and development and project management, data quality management, ICT continuity management, ICT reporting and internal ICT audit.