Executive summary

Belgium hosts a number of significant financial market infrastructures (FMIs), custodians and payment service providers, as well as critical service providers, some of which also have international systemic relevance. This Financial Market Infrastructures and Payment Services Report aims to provide a comprehensive overview of the oversight and supervision exercised by the National Bank of Belgium (the Bank) over these systems and institutions headquartered in or relevant for Belgium.

In addition, the report contains an overview of the regulatory changes with regard to these systems and institutions.

The oversight framework applicable to Swift is currently being reviewed by the Bank, in order to ensure that it reflects substantial evolutions in the regulatory and supervisory environment for FMIs.

A new oversight framework for payment instruments, schemes and arrangements (the PISA Framework), designed to foster improvements in the soundness and efficiency of electronic payments, has also been put into operation. Bancontact is amongst the payment instruments, schemes and arrangements to which this new framework is being applied in a first wave; it will be extended to Mastercard in 2024.

In 2023, the European Commission issued proposals for a new version of the Payment Services Directive (PSD3) and a Payment Services Regulation (PSR). While initiated in 2023, work continued under the Belgian presidency of the Council of the European Union in the first half of 2024.

Payconiq International SA, a payment institution active in several European countries, changed its governance structure, which led to the licensing of Bancontact Payconiq NV as a Belgian payment institution in 2023. The company has a significant share of the Belgian mobile payments market, in addition to its activities as the governance authority for the Belgian card payment scheme Bancontact.

This year's report focuses on different types of risks, such as geopolitical risk, operational risk, including ICT and cyber risk, and environmental and climate-related risks.

Sanctions against Russia and Russian countermeasures

Over the course of 2022 and 2023, the Bank closely monitored the impact of the geopolitical crisis that resulted from Russia's invasion of Ukraine. Since the invasion, several countries have imposed sanctions on Russian organisations and citizens. These sanctions, as well as Russia's countermeasures, have had an impact on some of the institutions subject to oversight and supervision by the Bank. Euroclear Bank, for example, had to manage increased risks resulting from international sanctions and Russian countermeasures.

Digital operational resilience

In order to guarantee financial stability, critical systems and institutions concerned by this report need to manage their operational risks – including ICT and cyber risks – carefully. Digital operational resilience was therefore once again one of the Bank's top priorities in 2023.

At EU level, the Digital Operational Resilience Act (DORA) entered into force on 17 January 2023 and aims to mitigate the risks associated with the digital transformation of the financial industry by imposing strict common rules. These rules apply to a wide range of financial institutions, plus critical ICT third-party service providers, for example cloud service providers, subject to a form of EU oversight.

The increased use of technology creates not only risks but also business opportunities for some entities. Emerging technologies such as distributed ledger technology (DLT) are being closely monitored by the authorities to assess their potential impact on financial stability. The EU Markets in Crypto-Assets Regulation (MiCA), for example, seeks to ensure a level playing field in terms of consumer protection, market integrity, financial stability, monetary policy transmission and monetary sovereignty. In October 2021, with these concerns in mind, the Eurosystem launched the investigation phase for a central bank digital currency (CBDC). In October 2023, the European Central Bank's (ECB) Governing Council decided to move to the preparatory phase.

An article focused specifically on this topic explains further how the Bank helps financial entities strengthen their capabilities to defend themselves against cyber threats.

Environmental and climate-related risks

Environmental and climate-related risks are another type of risk to which the Bank and the wider community have been paying increasing attention. While FMIs, custodians and payment service providers, as well as critical service providers, may not be exposed to such risks in the same way as, for example, insurers that cover damage caused by extreme weather events, physical risks posed by natural disasters and extreme weather events interrupting the services they or their service providers deliver are identified as an environmental and climate-related risk category. A themed article in this report provides an update on this type of risk in the FMI landscape.