Financial Market Infrastructures and Payment Services Report 2024

National Bank OF BELGIUM
Eurosystem

Financial Market Infrastructures and Payment Services Report 2024

National Bank OF BELGIUM
Eurosystem

Contents

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.

1. The Bank's role in oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and critical service providers

To give more insight into the systems and institutions providing payment, clearing, settlement, custody and other services, either from a wholesale or a retail market perspective, section 1.1 presents an overview of their structure and mutual interdependencies. Relevant processes and flows are explained in more detail in the subsequent parts of this report (i.e. chapters 2, 3 and 4). Meanwhile, section 1.2 explains the Bank's mandate and its role in the oversight and prudential supervision of this sector, from both a national and an international perspective.

1.1 Critical links in the functioning of financial markets and payment services

The systems and institutions covered in this report can be divided into three categories based on the type of services they provide: (1) securities clearing, settlement and custody, (2) payments, and (3) other financial infrastructure service providers. Through their activities or services for the financial industry, these systems and institutions are the critical links in the functioning of financial markets and payment services and of the real economy. When designed safely and managed properly, they can be instrumental in reducing systemic risks and contagion in the event of financial crises. At the same time, they are interlinked with other financial market infrastructures (FMIs), financial intermediaries and other actors such as merchants or retail customers. These interdependencies are briefly presented and illustrated in Figure 1.

Securities clearing, settlement and custody

Financial instruments are traded between buyers and sellers at an agreed price and contract terms. Trading in such instruments can take place either on-exchange (i.e. on a centralised platform designed to optimise the price discovery process and to concentrate market liquidity) or on an over-the-counter (OTC) basis (i.e. counterparties make bids and accept offers to conclude contracts directly among themselves). The final investor uses a custodian bank, which may rely on other intermediaries (e.g. brokers) to conduct trades. Exchanges such as Euronext Brussels are supervised by securities regulators and are not covered by this report.

FMIs and financial institutions that provide securities clearing, settlement and custody services are part of the post-trade securities landscape. The clearing of a trade via a central counterparty (CCP) generally means that the CCP becomes the buying counterparty for the seller and the selling counterparty for the buyer. Both original counterparties to the trade then have a claim on the CCP. The CCP's direct participants – usually banks or investment firms – are called clearing members. A clearing member may clear not only its own trades via the

CCP, but also those of its clients. There are no CCPs established in Belgium, but CCPs in other countries may be systemically important due to the clearing activities they provide for the Belgian securities market.

After clearing, the settlement of a trade entails a transfer of cash and/or a financial instrument between the parties on the books of a central securities depository (CSD). When a CCP has intervened to clear a trade, settlement takes place on the books of the CSD between the buyer and the CCP, and between the seller and the CCP. There are three CSDs established in Belgium : Euroclear Bank (an international CSD or ICSD), Euroclear Belgium and NBB-SSS. The settlement of the cash leg of a securities transaction takes place either through payment systems operated by central banks (i.e. central bank money, for example T2)[1] or on the books of an (I)CSD with banking status providing (multicurrency) cash accounts (i.e. commercial bank money, for example Euroclear Bank).

Financial institutions that facilitate their clients' access to securities investment markets are referred to as custodians. In that intermediary capacity, custodians can offer their clients safekeeping and settlement services. A local custodian primarily focuses on serving a single securities market. If a custodian has access to markets worldwide, it is considered a global custodian.

Payments

The payments landscape covers both wholesale payments (i.e. transactions between banks for institutional investors) and retail payments (i.e. transactions between retail customers) and includes payment systems, payment service providers (PSPs), such as payment institutions (PIs) and electronic money institutions (ELMIs), processors for retail payment instruments and card payment schemes.

Payment systems encompass large-value payment systems (LVPS) and retail payment systems (RPS). While LVPS generally exchange payments of very large amounts, mainly between banks and other participants in the financial markets, RPS typically handle a large volume of payments of relatively low value by means of credit transfers and direct debits. In Belgium, most interbank payments are processed by T2, the LVPS connecting Belgian banks with other European banks, and by the Centre for Exchange and Clearing (CEC), the retail payment system for domestic payments.

The role of PIs and ELMIs in the retail payments area is multi-faceted and growing. PIs and ELMIs have long been active in the card payment business, issuing payment cards to users and/or acquiring the funds for payments on behalf of merchants. The revised Payment Services Directive (PSD2) has further strengthened the role of non-banks in the market since they are now allowed (under certain conditions) to make use of the banking industry's accounting ledger to access and consult online the accounts of users of payment services.

Payment cards remain the most widely used type of payment instrument in Belgium and typically involve a four-party system, i.e. the cardholder (the payer), the card issuer, the merchant and the acquirer. In such a transaction, the card of the purchaser (the cardholder) is issued by an institution (the card issuer), which has traditionally been a bank but can also be a PI or an ELMI. The acquirer is in charge of "acquiring" the transaction on behalf of the merchant (i.e. performing all steps necessary for the purchaser's money to be transferred to the merchant's account). The relevant rules and conditions according to which (credit or debit) card payments can take place are defined by card payment schemes. The Belgian domestic (debit) card payment scheme is Bancontact. Mastercard Europe (MCE), established in Belgium, is the European subsidiary of the Mastercard group, which operates the international (credit) card payment scheme.

For Bancontact, a scheme switch is in place, but a single processor provides the underlying network and services for the majority of card payments, namely equensWorldline SE. For Maestro, the processing network is

1 On 20 March 2023, the new payments system T2 went live, replacing TARGET2. For more information, see https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html.

provided directly by Mastercard. After processing, card payment transactions are sent to the CEC for clearing and settlement. PIs also play a major role in providing money remittance services (fund transfers), allowing retail customers to transfer funds from Belgium to parties in locations around the world and *vice versa*.

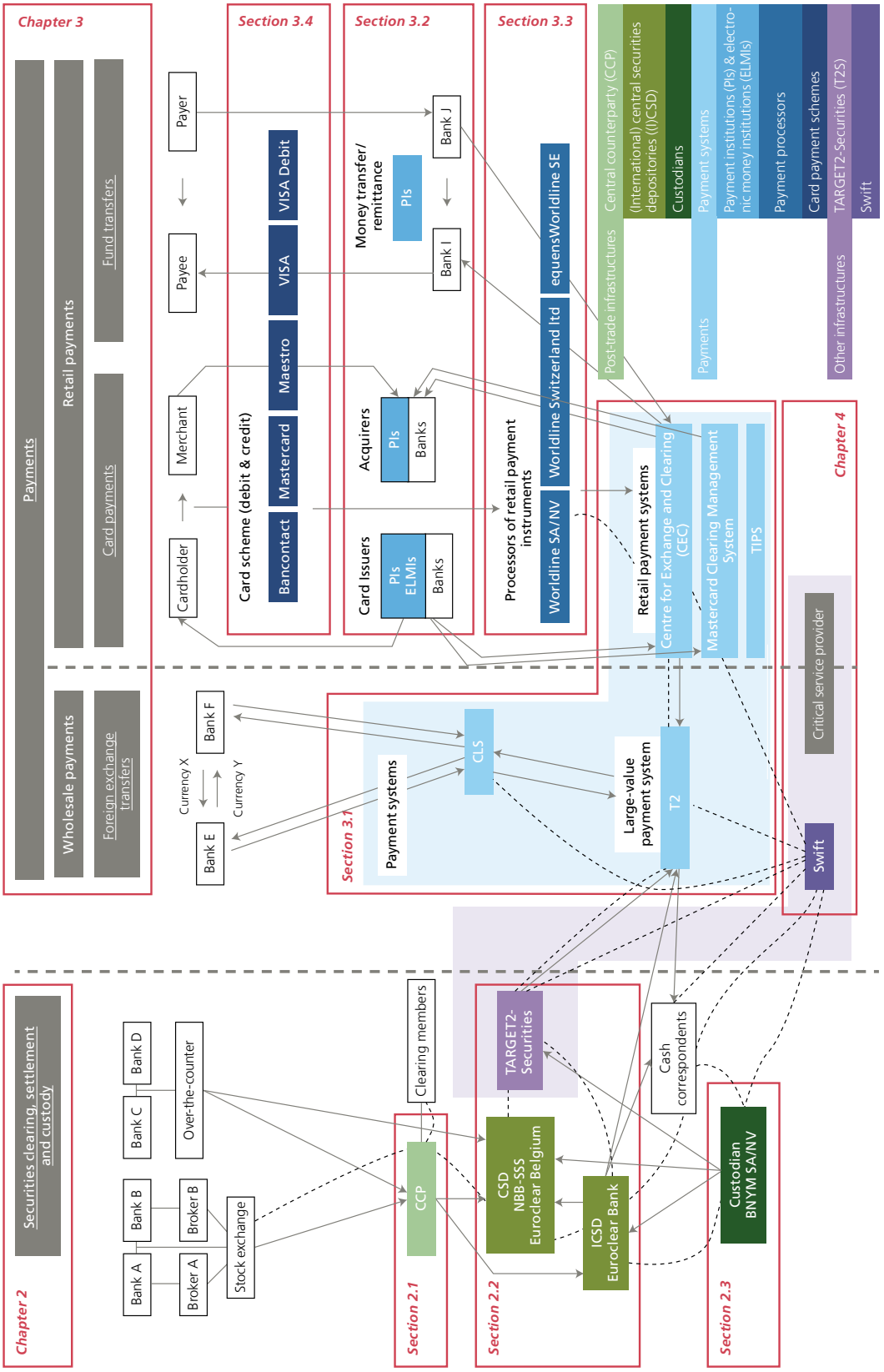
CLS, a settlement system for foreign exchange (FX) transactions, is linked to the LVPS operated by central banks for eighteen currencies (including T2 for the euro), making it possible to settle both legs of an FX transaction at the same time. CLS eliminates FX settlement risk arising for example from time zone differences, such as when a party transfers a currency it sold but does not receive concomitantly from the counterparty the currency it purchased.

Other infrastructures and service providers

TARGET2-Securities (T2S) is the common settlement platform for European CSDs. Although the messaging service provider Swift is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for daily financial messaging. It is therefore considered a critical service provider.

Figure 1

Connections between financial market infrastructures, custodians, payment service providers and critical service providers relevant for Belgium



1.2 FMIs, custodians, payment service providers and critical service providers subject to oversight and prudential supervision by the Bank

The Bank has responsibilities for both oversight and prudential supervision of FMIs, custodians, PSPs, such as PIs and ELMIs, and critical service providers.

The oversight and prudential supervision of FMIs vary in certain respects, ranging from the object, the competent authority, the areas covered, and the regulatory framework and tools used. However, both oversight and prudential supervision activities, and the framework they rely on, evolve over time.

Central banks have always had a close interest in the safety and efficiency of payment, clearing and settlement systems. One of the principal functions of a central bank is to ensure public confidence in money, which depends crucially on the ability of economic agents to transmit money and financial instruments smoothly and securely through payment, clearing and settlement systems. These systems must therefore be strong and reliable, available even when the markets around them are in crisis, and must never themselves be the source of such turmoil. The central bank's oversight of FMIs pursues these objectives by monitoring and assessing systems and, where necessary, inducing change. This is generally recognised as a core responsibility of central banks.

The Bank's oversight of payment, clearing and settlement systems is based on Article 8 of its Organic Act[1] and focuses on systems established in or relevant for Belgium. Although Swift is not a payment, clearing or settlement system, many such systems use it, effectively making it a critical service provider of systemic importance. Swift is therefore subject to a (cooperative) central bank oversight arrangement, with the Bank as lead overseer.

The Bank is also the prudential supervisory authority for individual financial institutions, as well as custodians and payment service providers. While significant credit institutions, such as The Bank of New York Mellon SA/NV (BNYM SA/NV), are directly supervised by the Single Supervisory Mechanism (SSM), less significant institutions remain under the prudential supervision of the Bank as the national competent authority.

Some FMIs are subject to both oversight and prudential supervision, typically if they have the status of a bank (as is the case for Euroclear Bank). Worldline SA/NV is also subject to both prudential supervision (as a payment institution) and oversight (as a retail payments processor). In such cases, oversight and prudential supervision complement one another: while oversight focuses on the sound functioning of the settlement system (by assessing compliance with oversight standards such as the CPMI-IOSCO Principles for financial market infrastructures or PFMI), prudential supervision focuses on the financial soundness of the operator (by assessing compliance with prudential legislation). As a result, oversight and prudential supervision typically cover different topics or assume different perspectives.

Oversight may focus on areas concerning the functioning of the system and how its organisation and operation minimise or avoid risks not only for itself but – just as importantly – for its participants. Examples include settlement finality rules, which reduce the risks associated with a participant's insolvency (i.e. to prevent the automatic unwinding of other participants' transactions with a bankrupt participant); delivery-versus-payment (DVP) or payment-versus-payment (PVP) mechanisms, which eliminate principal risks in transactions between participants; fair and open access for participants; and the stringent requirements for business continuity plans to ensure the continuity of services for participants. Oversight also takes into account risks related to system interdependencies (via connected systems or participants) that could trigger contagion risks in financial markets.

1 Article 8 of the Act of 22 February 1998 establishing the organic statute of the National Bank of Belgium, *Moniteur belge/Belgisch Staatsblad* 28 March 1998, 9.377.

Prudential supervision seeks to ensure that financial institutions are sound, thereby helping to maintain trust in these institutions and promote financial stability. Some types of risks are monitored by both FMI overseers and bank supervisors, albeit from a different perspective, as an FMI's business model is based on transferring liquidity (which has an element of time criticality) between – or on behalf of – its participants, whereas a bank's business model tends to be based on maturity transformation (short-term deposits into long-term assets). The regulatory approach to credit, liquidity and operational risk for FMIs therefore differs from that used for banks.

Due to such differences in scope, oversight and prudential supervision rely on different frameworks. For oversight, the PFMI cover payment systems, securities settlement systems, CSDs, CCPs and trade repositories, as well as critical service providers (see Annex F to the PFMI). When it comes to the implementation of these principles, further clarity is provided by guidelines, such as the CPMI-IOSCO Guidance on cyber resilience for FMIs or the Guidance on resilience and recovery of CCPs. In addition, the CPMI has published an analytical framework for distributed ledger technology in payment, clearing and settlement.

The tools used to conduct oversight and prudential supervision may differ, too. Oversight is generally based on principles and guidelines designed at the international level (e.g. the Eurosystem, CPMI, CPMI-IOSCO). The traditional approach to enforcement has been to urge FMIs and other (critical) service providers to adhere to these principles via central bank moral suasion (the so-called "soft law" approach). The requirements for prudential supervision, on the other hand, have been laid down in a legal framework that takes the form of EU directives and regulations and national legislation (the so-called "hard law" approach). However, over time, central bank oversight has become more formal, owing to the expanding role of the private sector in providing payment and settlement systems, as well as the growing criticality of the proper functioning of these systems. In an increasing number of areas, a hard law approach is being applied to oversight, as illustrated, for example, by the ECB Regulation on oversight requirements for systemically important payment systems (SIPSR) and the 2017 Belgian legislation on systemically relevant processors of retail payment instruments. In addition, the EU transposed the oversight framework for CCPs and CSDs (i.e. the PFMIs) into law in 2012 and 2014 (via EMIR[1] and the CSDR[2]). The Bank has been designated the competent supervisory authority for Belgian (I)CSDs and, as overseer, is also considered the relevant authority under the CSDR[3].

In order to pool expertise, reinforce synergies and align approaches between oversight and prudential supervision of FMIs, custodians, PSPs and other (critical) service providers, these two roles have been integrated into the same department within the Bank.

Table 1 below provides an overview of the systems and institutions supervised and/or overseen by the Bank. In addition to classification based on the type of services provided, these systems and institutions have been further grouped according to: (1) the type of role played by the Bank (prudential supervisor, overseer or both) and (2) the system/institution's international dimension (whether the Bank acts as the sole authority, as the lead authority in an international cooperative arrangement, or in another capacity). For systems and institutions governed by Belgian law and which are systemically relevant in the financial markets of other jurisdictions, or for the financial industry as a whole, the Bank cooperates with other authorities.[4] Such cooperation may involve multilateral arrangements in which the Bank acts as lead overseer (e.g. Euroclear, Swift). The Bank also takes part in a number of international cooperative arrangements (e.g. CCPs, BNYM, T2, T2S and CLS) in which another national authority acts as lead overseer/supervisor. Domestically, the Bank cooperates with the FSMA which has responsibilities for the supervision of financial markets with regard to the conduct of business rules. Annex 2 illustrates the organisational structure of FMIs with an international dimension governed by Belgian law.

1 European Market Infrastructure Regulation (EMIR), Regulation (EU) No 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs.

2 Regulation (EU) No 909/2014 of 23 July 2014 on improving securities settlement in the EU and on CSDs and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

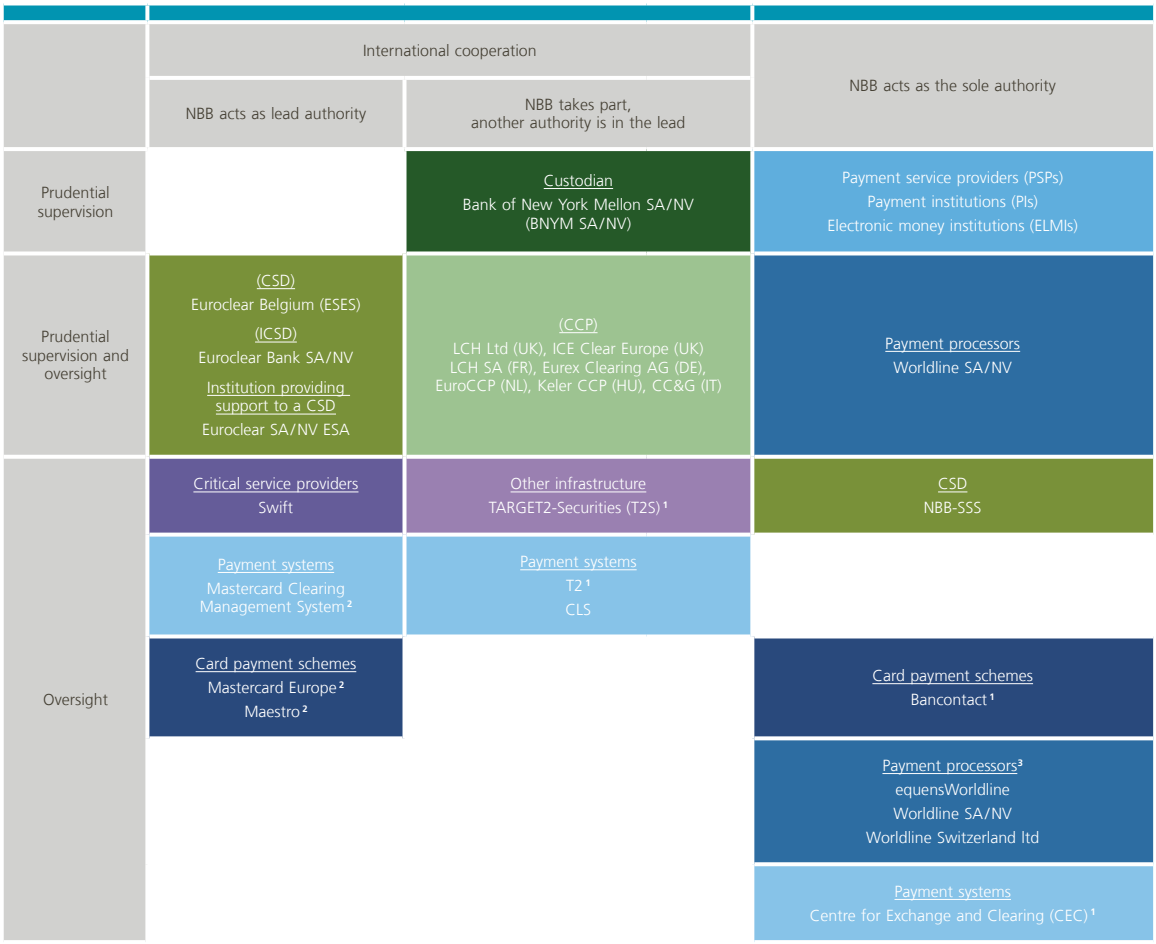
3 The FSMA has been designated, together with the Bank, as the national competent authority for CCPs under EMIR.

4 In line with CPMI-IOSCO Responsibility E (Cooperation with Other Authorities). By means of this report, the Bank intends to provide information to other authorities with which it does not engage in formal cooperation but which may be interested in understanding the applicable framework, regulatory approach and main supervisory priorities.

Table 1

The Bank's oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and other market infrastructures and critical service providers

(January 2024)



Source: NBB.

1 Peer review in Eurosystem/ESCB.

2 The NBB and the ECB act jointly as lead overseers.

3 Only for certain Belgian activities – Act of 24 March 2017 on the oversight of payment processors.

2. Securities clearing, settlement and custody

FMIs and financial institutions that provide securities clearing, settlement and custody services are part of the post-trade securities landscape. Systems that clear trades conducted on a stock exchange or concluded between counterparties on the OTC market, and systems that settle the obligations of the buyer and seller of a trade, are subject to oversight. In the EU, institutions that operate these systems are subject to supervision under EMIR and the CSDR. Figure 2 sets out the scope of the Bank's oversight and supervision for CCPs (section 2.1), (I)CSDs (section 2.2) and custodians (section 2.3).

The scope of the activities of (I)CSDs governed by Belgian law vary. While Euroclear Bank provides services covering a wide range of securities, Euroclear Belgium primarily provides services for Belgian equities. Under the CSDR, the Bank has been designated the sole competent supervisory authority[1] for Euroclear Bank and Euroclear Belgium and is also considered the relevant overseer for purposes of this directive. NBB-SSS, which is subject to oversight only, holds and settles public sector debt, including securities issued by the Belgian federal government and by regional or local governments, and private sector debt issued by corporate borrowers, credit institutions and other entities.

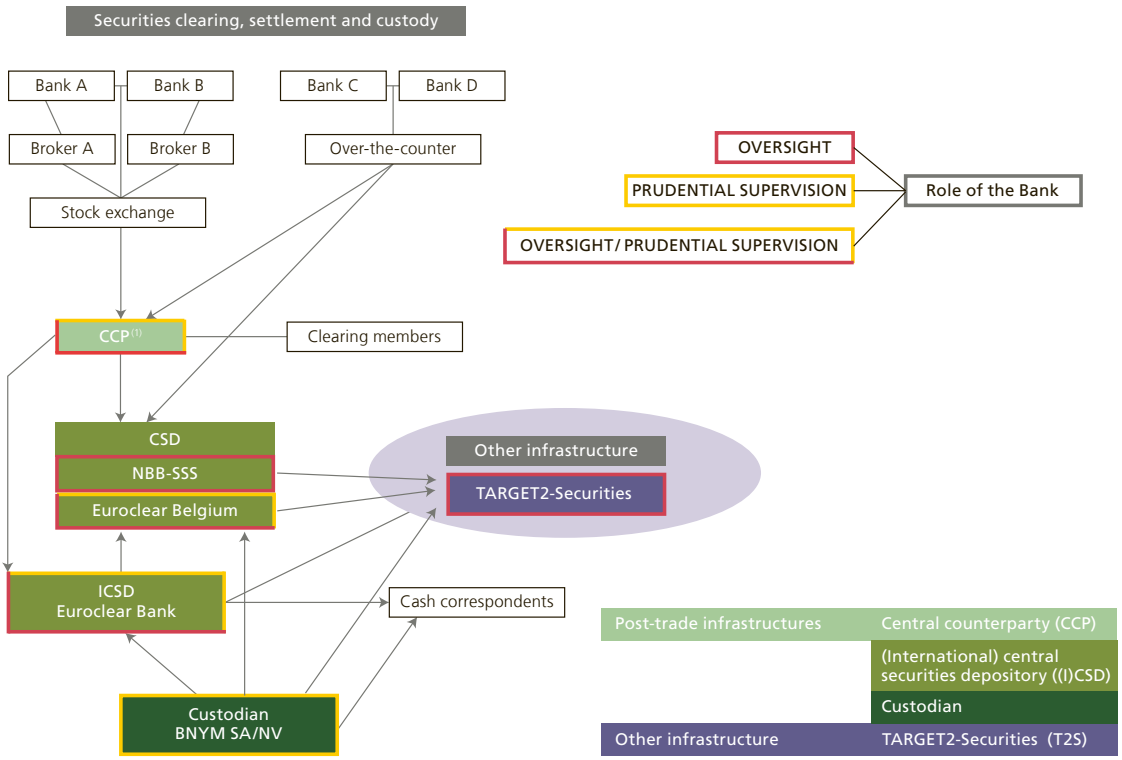
The daily settlement operations of Euroclear Belgium and NBB-SSS are outsourced to TARGET2-Securities (T2S), as is the case for other CSDs in Europe. T2S is not a CSD, but as it provides settlement services to many euro area and some non-euro area CSDs, it is essential that it enable participating CSDs to comply with the regulations applicable to them. The oversight of T2S is conducted by the Eurosystem. In line with PFMI Responsibility E (Cooperation with other authorities), the Eurosystem set up the T2S Cooperative Arrangement to ensure the involvement of all authorities with a legitimate interest in the smooth functioning of T2S, including the CSD oversight and market authorities that signed the T2S Framework Agreement, in coordination with the ECB and ESMA. The authorities monitor both the general organisation of T2S as a critical infrastructure (i.e. the technical platform, legal basis, governance structure and comprehensive risk management framework) and the services it provides, against an applicable PFMI subset. The Bank participates in this cooperative arrangement.

BNYM SA/NV is a global custodian established in Belgium with links to multiple (I)CSDs allowing its clients to hold securities issued in markets worldwide. BNYM SA/NV provides custody services (i.e. securities safekeeping, settlement and investor services) and is supervised by the ECB under the SSM as a significant credit institution.

1 For the following aspects, the Bank consults the FSMA, which remains the competent market authority: rules on conflicts of interest and record-keeping; requirements concerning participation; transparency; procedures for communicating with participants and other market infrastructures; protection of the assets of participants and their clients; freedom to issue securities via any CSD authorised in the EU; and access between a CSD and another market infrastructure.

Figure 2

Scope of the Bank's oversight and prudential supervision role in the post-trade securities landscape



1 LCH Ltd (UK), ICE Clear Europe (UK), LCH SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT).

2.1 CCPs

Changes to the regulatory framework

There are no central counterparties (CCPs) located in Belgium but some foreign CCPs are used by Belgian financial institutions for clearing, or they themselves use Belgian FMIs for settlement. The Bank therefore closely monitors regulatory developments relating to CCPs. The framework that regulates CCPs, i.e. their resilience and recovery and ultimately their resolution, was being further completed at the time of writing.

In September 2023, the FSB held a consultation on a draft report regarding financial resources for CCP resolution.[1] The report analyses the benefits and limitations of potential financial resources and tools for the resolution of systemically important CCPs and proposes specific tools and resources that should be placed at the disposal of the resolution authority.

In August 2023, the CPMI and IOSCO published a report on CCP practices to address losses arising from non-participant default events via recovery or orderly resolution tools.[2] This report could lead to further guidance under the PFMI for CCPs and other FMIs.

1 See https://www.fsb.org/2023/09/financial-resources-and-tools-for-central-counterparty-resolution-consultation-report/.
2 Available at https://www.bis.org/cpmi/publ/d217.htm.

Continuing their review of margining practices, the CPMI and BCBS issued a consultative report in January 2024, evaluating good practices and the transparency of initial margin in centrally cleared markets.[1] A CPMI-IOSCO discussion paper on streamlining variation margin processes in centrally cleared markets followed in February.[2]

In February 2024, the European Parliament and the Council reached a compromise on the third review of EMIR.[3] Through the introduction of a so-called "active account" requirement, the EU co-legislators require clearing by EU CCPs of categories of derivatives deemed substantially systemic (e.g. interest rate swaps denominated in euro and zloty and short-term interest rates in euro), although to a minimal extent. The requirement applies to entities that pass a *de minimis* threshold of clearing activity in the relevant contracts. Regarding supervision, the process to authorise the extension of CCP activities will become shorter. While the national competent authority (NCA) retains supervisory decision-making powers, ESMA powers are enhanced, including via an increase in the number of instances in which it can provide an opinion on NCA authorisations and decisions and the ability to participate in on-site inspections of CCPs. ESMA will also get enhanced coordination powers where more than one CCP is in an emergency situation.

The Commission published further implementing legislation[4] for the EU Regulation on CCP recovery and resolution (CCP-RRR) which sets out a framework for the recovery and resolution of EU CCPs. Moreover, ESMA has published guidelines on practices to determine when a CCP is deemed to be failing or likely to fail, the method to value contracts to be terminated, and the functioning of the CCP resolution college.[5]

Prudential and oversight approach

As required under European legislation, the Bank participates in five EU CCP supervisory colleges (see Table 2) that are relevant for Belgian markets, participants or CSDs. Post-Brexit, the Bank also takes part in the UK CCP colleges of LCH Ltd and ICE Clear Europe Ltd which are, however, no longer EMIR supervisory colleges.

Priorities for the ongoing supervision of EU CCPs are set by NCAs, after consultation with the college members. New CCP services or products, significant risk model changes and recovery plans are approved by the CCP's NCA, further to the opinion of the CCP's supervisory college.

As envisaged by the CCP-RRR, national legislators must designate a CCP resolution authority. Most authorities have established a sub-CCP-RRR resolution college and a first iteration of the CCP's resolution plan has been presented or approved. To date, the Bank participates in five EU CCP resolution colleges (see Table 2).

1 See https://www.bis.org/bcbs/publ/d568.htm.
2 See https://www.bis.org/cpmi/publ/d221.htm.
3 See https://www.consilium.europa.eu/en/press/press-releases/2024/02/07/capital-markets-union-council-an-parliament-agree-on-improvements-to-eu-clearing-services/.
4 See https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/ccp-recovery-and-resolution-regulation.
5 See https://www.esma.europa.eu/publications-and-data/guidelines-recommendations-and-technical-standards.

Table 2

Overview of CCP supervision and resolution of EU and third-country CCPs and NBB involvement

EU CCPs	Third-country CCPs	UK CCPs
EMIR		*UK EMIR legislation*
NCA supervision	ESMA supervision (second level)	Bank of England supervision
ESMA CCP supervisory committee Participation by CCP NCAs of existing EU CCPs	ESMA CCP supervisory committee Participation by CCP NCAs of existing EU CCPs	
EMIR supervisory college Participation in the college is mandatory NBB participates in the colleges of LCH SA (FR), Eurex Clearing (DE), Euronext Clearing (IT), Cboe Clear Europe (NL), and Keler CCP (HU)	EMIR college for third-country CCPs Participation in the college is voluntary The college functions as a channel for the exchange of information	Global CCP college *Basis: CPMI-IOSCO PFMI Responsibility E* Participation in the college is voluntary NBB participates in the colleges of LCH Ltd and ICE Clear Europe Ltd
CCP Recovery and Resolution Regulation (CCP-RR)		*UK CCP resolution regime code of practice*
National resolution authority of EU CCP		Bank of England acts as CCP resolution authority
ESMA CCP resolution committee Participation by national resolution authorities of EU CCPs		
CCP-RRR resolution college Participation in the college is mandatory NBB participates in the colleges of LCH SA (FR), Eurex Clearing (DE), Euronext Clearing (IT), Cboe Clear Europe (NL), and Keler CCP (HU)		UK CCP crisis management group *Basis: FSB Guidance on CCP Resolution and Resolution Planning*
NBB participates	NBB does not participate	

Source: NBB.

2.2 (I)CSDs

Changes to the regulatory framework

On 27 December 2023, Regulation (EU) 2023/2845 was published in the Official Journal of the European Union, amending the CSDR. This regulatory fitness and performance (REFIT) exercise was conducted mainly over 2022 and 2023 and introduces changes to the settlement discipline regime, the review and evaluation procedure, the passporting process, the regime for third-country CSDs and the provision of banking-type ancillary services, amongst other areas.

Under the amended CSDR, a supervisory college will be established for CSDs that are of substantial importance to the functioning of securities markets and the protection of investors in at least two EU member states. ESMA has been mandated to develop new regulatory technical standards to determine the criteria under which the activities of a CSD in a host member state could be considered to be of substantial importance to the functioning

of the securities markets and the protection of investors in that state and to submit them to the European Commission by mid-January 2025. Competent authorities have until one month after the entry into force of these regulatory technical standards to establish a college of supervisors.

The Bank expects that Euroclear Bank will meet the criteria in at least two member states, given its international profile and, in particular, its settlement activity in EU markets. Therefore, a supervisory college will have to be established. The Bank already hosts an annual forum at which the results of the review and evaluation of Euroclear Bank are presented to the competent authorities of the member states for which Euroclear Bank is of substantial importance for the functioning of the securities markets and the protection of investors under the currently defined criteria, as well as to ESMA and the EBA.

Prudential and oversight approach

The CSDR requires the Bank, in its capacity as the NCA, to conduct an annual review and evaluation (Art. 22 CSDR) of Euroclear Bank and Euroclear Belgium. At the beginning of the review and evaluation process, the Bank consults other authorities as required ("relevant authorities" as defined in the CSDR), the FSMA and the competent authorities from countries in which the Euroclear group has a CSD. For Euroclear Belgium, the assessment is coordinated with those conducted by the French and Dutch authorities competent for Euroclear France and Euroclear Nederland, respectively, as the operations, governance and rulebooks of the three CSDs – collectively termed the ESES CSDs – are, to a large extent, aligned. For Euroclear Bank, the final outcome of the review and evaluation is shared with the competent authorities of the countries for which the ICSD is substantially important, as well as with the EBA and ESMA (see Box 1).

As Euroclear Bank is also subject to banking law, the Bank conducts an annual Supervisory Review and Evaluation Process (SREP) in conjunction with its CSDR review and evaluation. The Bank streamlines all assessment frameworks applicable to Euroclear Bank, meaning CSDR and PFMI principles and key considerations are taken into account in the SREP.

Following the UK's withdrawal from the European Union, Euroclear Bank had to be recognised by the Bank of England in order to continue to provide CSD services in the UK. As required by Article 25 of the UK CSDR, [1] a cooperative arrangement between the Bank of England and the supervisory authority of the non-UK CSD, in this case, the Bank, had to be established. A Memorandum of Understanding with the Bank of England was thus signed in January 2023, renewing a pre-existing cooperation arrangement.

1 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014, as amended and retained in UK law.

BOX 1

Cooperation between the Bank and other authorities with regard to Euroclear

The Bank cooperates with domestic and foreign authorities in the framework of the oversight and supervision of Euroclear entities governed by Belgian law, i.e. Euroclear SA, Euroclear Bank and Euroclear Belgium. The table below lists these authorities and the basis for a cooperation arrangement with them.

Cooperation	Basis for cooperation
National cooperation	
FSMA	Market authority responsibilities for (I)CSDs in Belgium
International cooperation	
Euroclear SA/NV	
Euroclear Group oversight auhtorities and market supervisors (BE: NBB, FSMA; FI: Bank of Finland, Finanssivalvonta; FR: Banque de France (BdF), Autorité des marchés financiers (AMF); NL: De Nederlandsche Bank (DNB), Autoriteit Financiële Markten (AFM); SE: Riksbank, Finansinspektionen; UK: Bank of England)	MoU on cooperation and information exchange concerning the relationship of Euroclear SA with the (I)CSDs of the Euroclear group; Euroclear SA is both the parent holding company and service provider to the Euroclear group entities
Euroclear Bank	
Central banks of issue of major currencies in Euroclear Bank (Federal Reserve System, BoE, BoJ, Reserve Bank of Australia and ECB as observer)	Multilateral oversight cooperation with the relevant central banks of issue of the major currencies settled in Euroclear Bank
European Central Bank	Bilateral oversight cooperation on specific aspects of Euroclear Bank relevant for euro area financial stability
Bank of England	Following the UK's withdrawal from the European Union, Euroclear Bank was recognised by the Bank of England in order to allow it to provide CSD services in the UK. As required by the UK CSDR, a cooperative arrangement between the Bank of England and the NBB was established
Bank of Japan	Bilateral oversight cooperation on specific aspects of Euroclear Bank relevant for Bank of Japan
Central Bank of Ireland	Bilateral cooperation with regard to the settlement of Irish bonds and, as of 2021, equities in Euroclear Bank
Hong Kong Monetary Authority	Bilateral oversight cooperation focusing on the links between Euroclear Bank and Hong Kong market infrastructures
Banque Centrale de Luxembourg (BCL) / Commission de Surveillance du Secteur Financier (CSSF)	Cooperation and communication arrangement on the oversight and prudential supervision of the ICSDs Euroclear Bank and Clearstream Banking SA (Luxembourg), under Responsibility E of the PFMI
Securities Exchange Commission (SEC)	Euroclear Bank operates under an SEC exemption that allows it to perform certain clearing activities for its US participants without having to register as a clearing agency with the SEC
ESES	
ESES overseers and market supervisors (BE: NBB, FSMA; FR: BdF, AMF; NL: DNB, AFM)	Multilateral cooperation covering the CSDs of Euroclear France, Euroclear Nederland and Euroclear Belgium sharing a common rulebook.

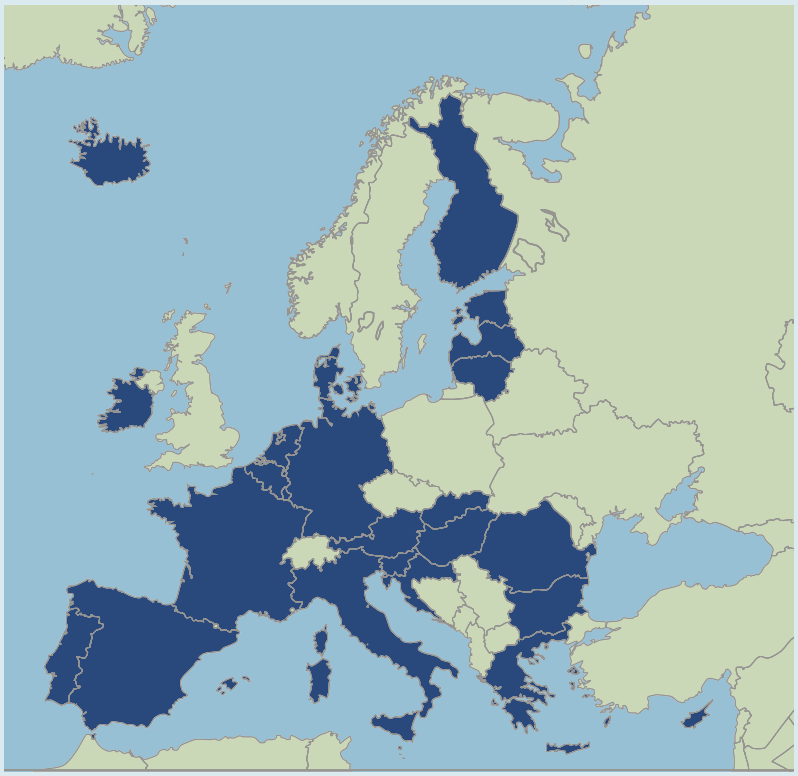
Source: NBB.

Under the CSDR, the Bank, as the competent authority, needs to involve other authorities in the supervision of (I)CSDs governed by Belgian law. The CSDR identifies as "relevant authorities" those responsible for oversight, central banks in the EU in whose books cash is settled, and central banks in

the EU issuing the most relevant currencies in which settlement takes place. In the case of Euroclear Bank and Euroclear Belgium, the Bank also acts as a relevant authority in its capacity as overseer of securities settlement systems. As Euroclear Belgium settles euros in central bank money, the Eurosystem (represented by the Bank) is also considered a relevant authority. The Eurosystem is likewise a relevant authority for Euroclear Bank, which also carries out settlements in euro.

In addition to the FSMA and the relevant authorities, the competent authorities from EEA countries in which Euroclear group has a CSD are involved in the annual review and evaluation process of Euroclear Belgium and Euroclear Bank. As shown in the map below, Euroclear Bank is of substantial importance for many EEA countries, [1] and the Bank shares an outcome report from this process with authorities in those countries.

EEA countries for which Euroclear Bank is of substantial importance



1 At the time of writing, Euroclear Bank was of substantial importance for Austria, Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain.

In 2023, a major crisis erupted when Credit Suisse lost the confidence of the markets. Given its commercial relationships with Credit Suisse, Euroclear Bank decided on a range of precautionary management actions before the Swiss authorities intervened to limit the potential impact. Not only was Credit Suisse a key participant in Euroclear Bank's securities settlement system, for both its own activities and those of its clients, but it was also, given its footprint in Switzerland, a regular treasury counterparty for short-term reinvestments in Swiss francs (CHF). It provided services as a cash correspondent in CHF within the Euroclear system, was responsible for the receipt of income and redemption payments related to Eurobonds in CHF and acted as a settlement bank for Swiss securities. From a risk management perspective, with Euroclear Bank accepting collateral for intraday cash lending to participants for settlement activity, the financial instruments of Credit Suisse were impacted by temporarily high haircuts. The cash correspondent was disabled and risk mitigating measures were taken across the Swiss link during the period of turbulence, which lasted until the acquisition of Credit Suisse by UBS eased tensions in the financial markets.

BOX 2

Risks incurred by Euroclear Bank due to sanctions against Russia and Russian countermeasures

At the start of Russia's war in Ukraine, the EU and other G7 members imposed a number of sanctions, impacting the assets of Russian entities such as the Central Bank of Russia and the Russian National Securities Depository (NSD). A large share of the assets affected by these sanctions were safeguarded and, following imposition of the sanctions, effectively frozen or immobilised in the accounts of Euroclear Bank. Euroclear Bank also safeguards international investors' assets on the Russian market, through its link with NSD. As a result of Russian countermeasures, these assets were also frozen in the accounts of Euroclear bank at NSD. Thus, Euroclear Bank has incurred a number of risks while implementing international sanctions against Russia and enduring Russian countermeasures.

A large share of the sanctioned assets in Euroclear Bank – predominantly fixed-income financial instruments – have reached maturity and been transformed into cash since the introduction of the sanctions. Given the high interest-rate environment in 2023, Euroclear Bank reported unexpected and extraordinary revenue from the reinvestment of sanctioned cash deposits. At the same time, its operating costs and risks have increased substantially given the challenges of managing an expanding balance sheet, the implementation of sanctions, and Russian countermeasures. Furthermore, various parties in Russia are contesting the consequences of application of the sanctions and are pursuing litigation against Euroclear Bank in Russia. They are seeking compensation for the frozen securities and cash held by Euroclear Bank as well for lost opportunities and damage.

Given the role played by CSDs in safeguarding the securities and cash of sanctioned participants, resulting in unexpected and extraordinary revenue from the re-investment of sanctioned cash of the Central Bank of Russia, the EU looked to these institutions in order to recover the net profits earned so as to provide financial support for Ukraine. A Council regulation,[1] adopted in February 2024, determined – as a first step – how this so-called windfall revenue of CSDs should be used. CSDs are now required to account

1 Regulation – EU - 2024/576 - EN – EUR-Lex (europa.eu).

separately for and manage revenue from the re-investment of sanctioned cash in their financial accounts and are prohibited from distributing any such profits as dividends. Additionally, CSDs must report annually to the Commission and the national supervisory authority on the total amount of such cash, revenue and windfall profits. These measures paved the way for a subsequent Council regulation [1] in May 2024, aimed at redirecting 99.7 % these net profits (the financial contribution) towards financing support for Ukraine. Nonetheless, the regulation acknowledges the existence of risks and costs endured by CSDs due to the implementation of international sanctions and therefore foresees that 10 %, or more in an emergency situation, of the financial contribution could be retained provisionally to comply with capital and risk management requirements. The Bank is closely monitoring the evolving risk environment facing Euroclear Bank due to the sanctions regime and associated countermeasures, especially given the systemic nature of Euroclear Bank and the potential for adverse effects on financial stability.

1 Regulation – EU - 2024/1469 - EN – EUR-Lex (europa.eu).

Cyber risk management remains a top priority for supervisors, particularly in the current geopolitical context. Euroclear Bank, Euroclear Belgium and NBB-SSS participated in the 2023 ESCB Cyber Assessment Survey, an assessment of the maturity of FMI cybersecurity, based on the June 2016 CPMI IOSCO Guidance on cyber resilience. The ESA Technical Forum, which is chaired by the Bank and includes central banks and the securities regulators for all Euroclear group CSDs, monitors the investments made at Euroclear group level to implement cybersecurity aspects of the group's strategy and further enhance system resilience. Cyber and operational risks are recurring topics as well as reasons for interaction with the Bank's risk management (second line of defence) and internal audit (third line of defence) services.

ESG (environmental, social and governance matters) is one of the pillars of the Euroclear group's strategy. The group's ESG policy is publicly available and built around the following axes: environment, workplace, community and governance. By focusing on these axes, the Euroclear group aims to support and enable a sustainable financial marketplace. At the same time, it recognises the existence of risks and, for example, requires Euroclear companies to identify and manage climate-related risks. [1] In 2023, the Bank conducted a first FMI-specific review of climate-related and environmental risks. Please see the relevant themed article in this report for more information on the Bank's work in this area as well as the lessons learned.

Although CSDs operated by members of the ESCB are exempt from the authorisation and supervision requirements of the CSDR, [2] some prudential requirements are nonetheless applicable to them. Under the regime for granting eligibility to securities settlement systems and links for their use in Eurosystem credit operations, based on the CSD's compliance with the CSDR requirements and in cooperation with the Eurosystem, the Bank exercises its overseer role by conducting an annual review and evaluation of NBB-SSS against the CSDR requirements that are relevant from a "user perspective". [3]

1 ESG group policy, Section 3.1.4.

2 Pursuant to Article 1(4) CSDR.

3 NBB-SSS is eligible for monetary policy operations by the Eurosystem. This means that the Eurosystem accepts securities as collateral in NBB-SSS. As the Eurosystem is effectively a user of NBB-SSS, it needs assurance that NBB-SSS is safe to use.

In 2023, the IMF carried out an FSAP in Belgium and, as part of its work, issued a detailed assessment report[1] on Euroclear Bank. The report looked at compliance by both Euroclear Bank and its supervisory authorities, i.e. the Bank and the FSMA, with the CPMI-IOSCO's Principles for financial market infrastructures (PFMI).

1 See https://www.imf.org/en/Publications/CR/Issues/2023/12/07/Belgium-Financial-Sector-Assessment-Program-Detailed-Assessment-of-Observance-Assessment-of-542179.

BOX 3

International dimension of Euroclear Bank

Due to the nature of its business model, Euroclear Bank has an international scope. This is illustrated, for example, by the participants, currencies and linked securities markets with which it works. At the end of 2023, Euroclear Bank had more than 1 800 participants. Its participant base consists mainly of non-domestic entities, including more than 40 CCPs and CSDs, as well as credit institutions, broker-dealers and investment banks.

Apart from its notary function for international bonds (Eurobonds), which it shares with Clearstream Banking SA (Luxembourg), Euroclear Bank aims to provide its participants with a single gateway to access many foreign securities markets (i.e. Euroclear Bank has a link with foreign CSDs which act as notaries for securities issued in their local markets). When (I)CSDs offer their participants access to foreign securities markets, they are considered investor (I)CSDs, while the foreign (I)CSDs are referred to as issuer (I)CSDs. Euroclear Bank is connected to more than 50 foreign CSDs as an investor ICSD in domestic markets.

To provide services in international bonds and a wide range of foreign securities, 100 different currencies are eligible in the system operated by Euroclear Bank. Securities can be settled against payment in a Euroclear settlement currency[1] (44 currencies) which may differ from the denomination currency.[2]

At the end of 2023, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to the equivalent of €18.3 trillion (up from €17.5 trillion in 2022). The euro is the main denomination currency (51%), followed by the US dollar (27%) and the pound sterling (11%). Fifty-four percent of securities deposits are in international bonds, for which issuers can choose the denomination currency and the governing law.

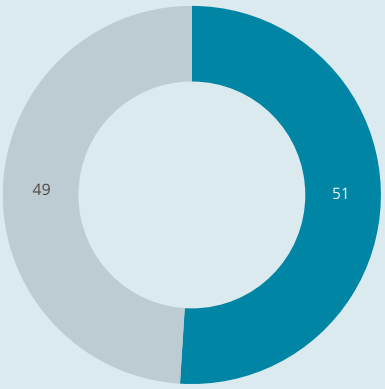
In terms of settlement turnover, the number of transactions settled in Euroclear Bank in 2022 came to 171 million (up from 163.3 million in 2021). In value terms, this represents € 727.7 trillion (up from € 692.2 trillion in 2021). 68 % of settlement turnover, free-of-payment and against-payment transactions, were denominated in euros, followed by 14 % in US dollars and 8 % in pound sterling. International debt accounts for 18 % of settlement turnover per security type, as compared to securities deposits, while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds.

1 A settlement currency is a currency in which cash settlement can take place.
2 A denomination currency is the currency in which a security is denominated. This currency is used as a unit of account for the nominal value of the security, but it is not necessarily used to settle the cash leg of transactions.

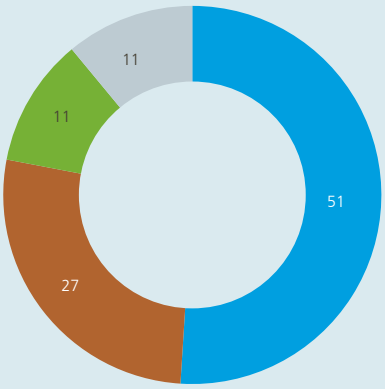
The interconnectedness of Euroclear Bank with other FMIs is a critical component of the Euroclear group's strategy to establish a common pool of collateral assets in which group entities provide collateral management services as a triparty agent assuming collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of a transaction between two participants. At the end of 2023, at group level, the average daily value of triparty collateral managed by Euroclear (I)CSDs reached the equivalent of € 1.67 trillion.

Composition of securities deposits and turnover (%, at the end of 2023)

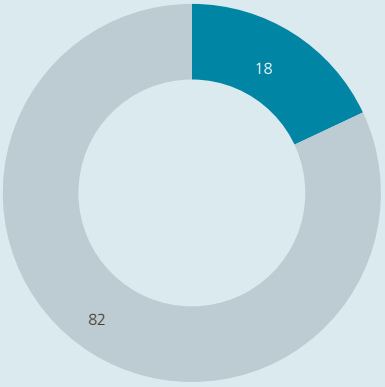
Securities deposits in value (%) - Breakdown by security type



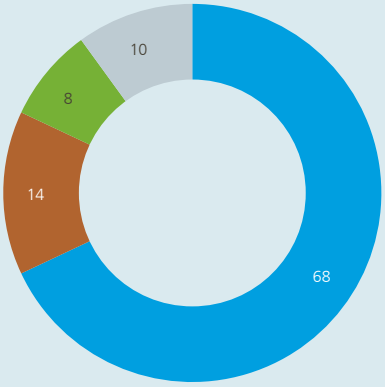
Securities deposits in value (%) - Breakdown by currency



Settlement turnover in value (%) - Breakdown by security type



Settlement turnover in value (%) - Breakdown by currency



International debt (incl. eurobonds)
Other securities (incl. domestic debt, equities, funds)

EUR
USD
GBP
Other

Source: Euroclear.

2.3 Custodians

Changes to the regulatory framework

In 2023, the regulatory framework applicable to custodians remained unchanged.

Prudential and oversight approach

BNYM SA/NV is a significant institution, meaning it falls under the direct supervision of the SSM. Supervisory work relating to the CRD/CRR framework is therefore carried out jointly by the Bank and the ECB within the SSM. BNYM SA/NV is also subject to monitoring by the Bank in terms of the specific requirements applicable to depository banks and client asset protection rules.

BNYM SA/NV is a subsidiary of BNY Mellon, a US-based global systemic bank. At the end of 2023, BNYM SA/NV had a German subsidiary and several branches in Europe through which it operates in local markets. BNYM SA/NV has branches in Luxembourg, Frankfurt, Amsterdam, Paris, Dublin, Milan, Madrid and Copenhagen and an operational branch in Poland.

BNYM SA/NV is the group's custodian for European clients and the European gateway to euro area markets and payment infrastructures within the BNYM group. BNYM SA/NV settles transactions in a wide range of currencies, primarily EUR, GBP, USD and JPY (see Box 4).

Due to the group's global organisational structure and specific mix of activities and operating model, governance and operational risk remained the main risk areas in 2023 and will continue to be of high importance in the 2024 review cycle. The group's remuneration policies and documentation were among the issues highlighted in the 2023 review and will continue to be points for attention in 2024 review work. The main areas of attention in terms of operational risk in 2023 were operational resiliency, outsourcing arrangements, and ICT and cyber risks. As a global custodian, the BNYM group operates according to a "follow the sun" model which enables it to process clients' transactions and related services around the globe continuously, across different time zones. To do so, BNYM SA/NV relies heavily on an (intragroup) outsourcing arrangement. Such a model can present advantages in terms of efficiency and resiliency (e.g. back-up locations), but it can also introduce organisational complexities and additional points for attention (such as the monitoring of outsourced activities). As a result, amongst the assessments carried out in 2023, the Bank scrutinised the outsourcing register and recovery plans and acted as an observer in a live default simulation exercise. The Bank will continue its assessment of business continuity and exit plans relative to outsourcing arrangements in 2024. An SSM-wide cyber stress test will also be carried out by the ECB in cooperation with the NCAs in 2024.

The level of market risk (including spread risk) and interest rate risk was another area for attention in the 2023 supervisory review cycle. In June 2023, the new EBA guidelines on interest rate risks in the banking book (IRRBB) entered into force. As part of the 2024 supervisory review and evaluation process (SREP), the JST will therefore perform a first-time challenge and assess BNYM SA/NV against these new guidelines.

Due to the high value of multi-currency transactions handled by BNYM SA/NV each day, the intraday management of both euro and non-euro currencies relating to credit and liquidity risks, as well as the risk control framework around credit risk (concentration), is of importance for BNYM SA/NV and will remain a point for attention in the supervisory review cycle. More information on the specific risk profile of custodian banks can be found in Box 5.

In recent years, the Bank contributed to the development of a dedicated assessment framework which can be used by banking supervisors to assess restitution risk[1][2] during their annual supervisory reviews. This framework will be structurally implemented within the SSM as from the 2024 supervisory review cycle. The importance of restitution risk increased over the past year in view of ongoing geopolitical tensions.

Last but not least, the Bank will continue to pay increasing attention to climate-related risks (see Chapter 8 on the monitoring of climate-related risks by financial market infrastructures, payment processors and financial messaging services). The JST will also continue to assess progress in the implementation of climate-related and environmental plans and the Bank's overall progress towards fulfilling ECB expectations.[3] In addition, the SSM will conduct a climate-related risk scenario analysis in 2024.

1 Restitution risk is the risk of an institution having to reimburse a client for the value of financial instruments held in custody if lost at or by a sub-custodian or CSD. This obligation arises from AIFMD/UCITS V.

2 See also the discussion of restitution risk in the 2023 FMI Report, available at https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2023/fmi-2023_dlt.pdf.

3 See https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf.

BOX 4

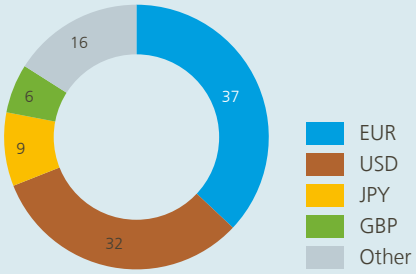
The international dimension of the Bank of New York Mellon and BNYM SA/NV

The Bank of New York Mellon, a banking group incorporated in the US, is the world's largest custodian bank in terms of assets under custody ($ 48 trillion as of December 2023, representing a year-on-year increase of 9 %). It is a global systemically important bank (G-SIB), providing asset and investment management services to institutional customers. The Bank of New York Mellon SA/NV (BNYM SA/NV), the group's Belgian subsidiary, primarily provides asset services and acts as the group's custodian for T2S markets and as the global custodian for EU customers. BNYM SA/NV has a non-bank subsidiary in Germany and branches in Luxembourg, the Netherlands, Germany, France, Ireland, Italy, the UK, Denmark and Spain through which it operates in these local markets; it also has an operational branch in Poland (with no access to the local market). BNYM SA/NV has been assessed by the Bank as an "other systemically important institution" (O-SII), based on the relevant EBA guidelines.

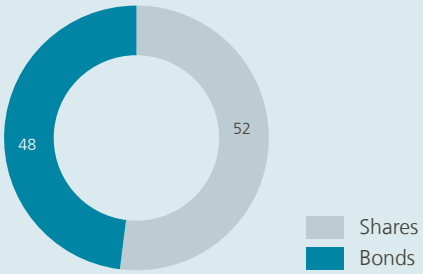
At the end of 2023, BNYM SA/NV served almost 4 500 international, institutional customers, on whose behalf it held the equivalent of € 3.1 trillion in assets under custody, denominated in more than 80 different currencies. Most of these assets are denominated in EUR (37 %), followed by USD (32 %), JPY (9 %) and GBP (6 %). Forty-eight percent (48 %) of the assets are bonds and 52 % are shares. In terms of settlement activity, BNYM SA/NV processed about 8.9 million transactions valued at the equivalent of € 66.7 trillion in 2023; the main transaction currencies were USD (62 %), EUR (27 %), GBP (9 %) and DKK (1 %).

Composition of assets under custody and turnover (%, end of 2023)

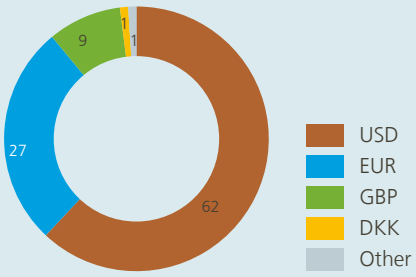
Assets under custody, per currency (%), end of 2023



Assets under custody, per security type (%), end of 2023



Settlement turnover value, per currency (%), 2023



Source: BNY Mellon.

BOX 5

Specific risk profile of custodian banks and limits on the calculation methods of CRR (Capital Requirements Regulation) risk ratios

The CRR's approach to risk and risk ratio calculation methods

Most financial institutions do not have direct access to central securities depositories (CSDs) – which provide notary services or provide and maintain securities accounts at the top-tier level – in all the markets in which they invest. Therefore, custodian banks establish such connections in multiple markets, hold their clients' assets in custody, and act as an intermediary between investors and CSDs in various markets. In keeping with this business model, which is crucial for the financial markets, custodians should seek to minimise the risks on their balance sheets. They are thus often perceived by clients as "safe havens". Widely used and trusted measures such as a (high) common equity tier 1 (CET1) ratio and (low) risk weighted assets (RWA) density tend to confirm that custodians are relatively risk averse and safe. This view is not misleading overall, but it should be nuanced and complemented by other metrics to provide an accurate reflection of the risk profile of custodians.

For example, geopolitical risks are rapidly and visibly increasing and impact financial institutions both on- and off-balance sheet. As such, they should be reflected in risk and capital ratios. For some institutions, however, such as custodian banks, the prudential capital requirements imposed by the Capital Requirements Regulation (CRR) do not increase commensurately along with an increase in risk; this is a direct consequence of the CRR risk ratio calculation methods, on the one hand, and the limited number or types of risks that are recognised by this regulation, on the other hand.

Indeed, certain risks that fall within the scope of the regulation are materially underestimated by the capital requirement calculation methods. In addition, material parts of in-scope risk categories are overlooked or disregarded. In the latter case, financial institutions do not have to cover these risks with regulatory capital. Such partially covered risks include credit risks to which institutions are exposed during the business day, also known as intraday credit risks, which are relatively material for custodians due to their settlement-related payment activities. The same holds true for interest rate risks related to positions in the banking book to which institutions are exposed: as these do not appear in the trading book, they are not covered by the regulatory capital requirements. Finally, specific risks that are common to custodians, such as restitution risk, simply fall outside the scope of the CRR.

Of course, custodian banks, conscious of their central and crucial role in the markets, do not ignore these types of risks and calculate a capital buffer under Pillar 2 to cover (most of) them. However, these calculations are specific to each institution. Understanding the specificities of these calculation methods requires cumbersome efforts by regulators, and their differences allow for limited comparability and benchmarking.

Relevance of interest rate risk in the banking book and restitution risk for custodians in the light of recent developments

Throughout 2022 and 2023, central banks around the world raised interest rates several times to tame above-target inflation rates. Along with the rates set by central banks, market interest rates started to shift, thereby increasing interest rate risks for financial institutions. In line with their business model – which entails safeguarding non-maturity wholesale deposits which can flow out instantly – custodian banks often avoid holding financial positions for trading purposes and instead hold substantial positions in order to maintain high-quality, readily available liquidity. These highly liquid securities are rightly not included in the trading book; however, an unfortunate consequence of this is that they are not covered by the regulatory capital requirements.

The recent increase in geopolitical risk has shown that, in certain cases, decisions may be taken to freeze the assets of a given account holder, issuer or country. In keeping with their business model, custodian banks may have close ties with CSDs or other intermediaries (global custodians or CSDs) that are the depositors of such securities or that are located in countries subject to sanctions. European directives protect investors against the loss of their financial assets, [1] irrespective of where they are held. Indeed, custodian banks, often referred to as depositary banks in this context, are liable for the restitution of these assets to their clients if they are lost. Although financial institutions are exposed to restitution risk, the CRR does not address this particular risk and thus does not provide for a market-wide regulatory capital calculation method.

The position and actions of the Bank

The Bank is of the opinion that financial markets are best protected when financial institutions mitigate all risks to which they are exposed through transparent, cross-cutting Pillar 1 coverage methodologies. Custodian banks, as explained above, are exposed to many risks for which the applicable legislation does not specifically require Pillar 1 capital. The Bank, as a competent supervisory authority, is striving to close this regulatory gap to the extent possible.

Competent authorities have a number of tools at their disposal to compensate for the imperfect coverage of the CRR, such as the possibility to impose more qualitative requirements or to slightly increase – within predefined limits – the amount of capital that financial institutions must set aside. Yet, ultimately, the aim should be to compel financial institutions to set aside the exact amount of capital necessary to cover their exposures.

This is why the Bank's team in charge of the supervision of custodian banks has contributed and continues to contribute decisively to the SSM working groups responsible for the development of new methodologies, raising awareness of these risks and proposing adequate, generally applicable calculation methods to more aptly cover the aforementioned risks with Pillar 1 capital.

1 Those that fall within the scope of AIFMD/UCITS V.

3. Payments

The Bank has broad responsibility in the payments sphere and acts as both overseer and prudential supervisor, as illustrated in Figure 3 below. These approaches are complementary: while oversight focuses on the sound and safe functioning of payment systems, payment instruments,[1] payment schemes[2] and other payment infrastructures, prudential supervision aims to ensure the safe, stable and secure provision of payment services to end users.

The interest of central banks in the payments sphere stems from a connection with various core tasks. Directly or indirectly, payment systems, instruments and services may affect the practical implementation of monetary policy, the financial stability of the country and confidence in its currency and can contribute to a safe, reliable and competitive environment.

Section 3.1 covers the two payment systems at the heart of the Belgian payments infrastructure: T2[3] and the Centre for Exchange and Clearing (CEC). T2 is the large-value payment system (LVPS) connecting Belgian banks with other euro area banks for the processing of payments and serves as the basic connecting infrastructure for the implementation of central bank monetary policy. The CEC is the domestic retail payment system (RPS) processing domestic payments between Belgian banks. In addition to T2, the Mastercard Clearing Management System operated by MCE (established in Belgium) was designated as a systemically important payment system (SIPS) by the ECB Decision of 4 May 2020 pursuant to Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2020/26).[4] This regulation lays down the – mainly quantitative – thresholds which, once exceeded, lead to designation of the entity concerned as a SIPS.

The Bank also participates in the cooperative oversight framework of CLS, a payment-versus-payment (PVP) settlement system for foreign exchange (FX) transactions. The US Federal Reserve is the lead overseer and supervisor of CLS. In addition, CLS is overseen by the Oversight Committee (OC), an international cooperative oversight arrangement comprised of the central banks whose currencies can be settled in CLS and five central banks from the euro area (including the Bank).

Section 3.2 deals with the prudential supervision of payment institutions (PIs) and electronic money institutions (ELMIs) – a part of the PSP sector which offers services that compete with those of incumbent PSPs (mainly banks). This type of non-bank PSP for retail payments provides payment services and issues, redeems and distributes electronic money. ELMIs may also provide payment services and, given their ability to issue electronic money to the public, are subject to a stricter prudential regime, such as more stringent capital requirements.

1 A payment instrument is an instrument to execute payments such as payment cards, credit transfers and direct debits.
2 A payment scheme is a set of rules, practices, standards and/or guidelines for the execution of payment transactions.
3 On 20 March 2023, the new payment system T2 went live and replaced TARGET2.
For more information, see https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html.
4 See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D0026(01)&from=EN.

As an acquirer[1] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in this respect are covered in section 3.3.

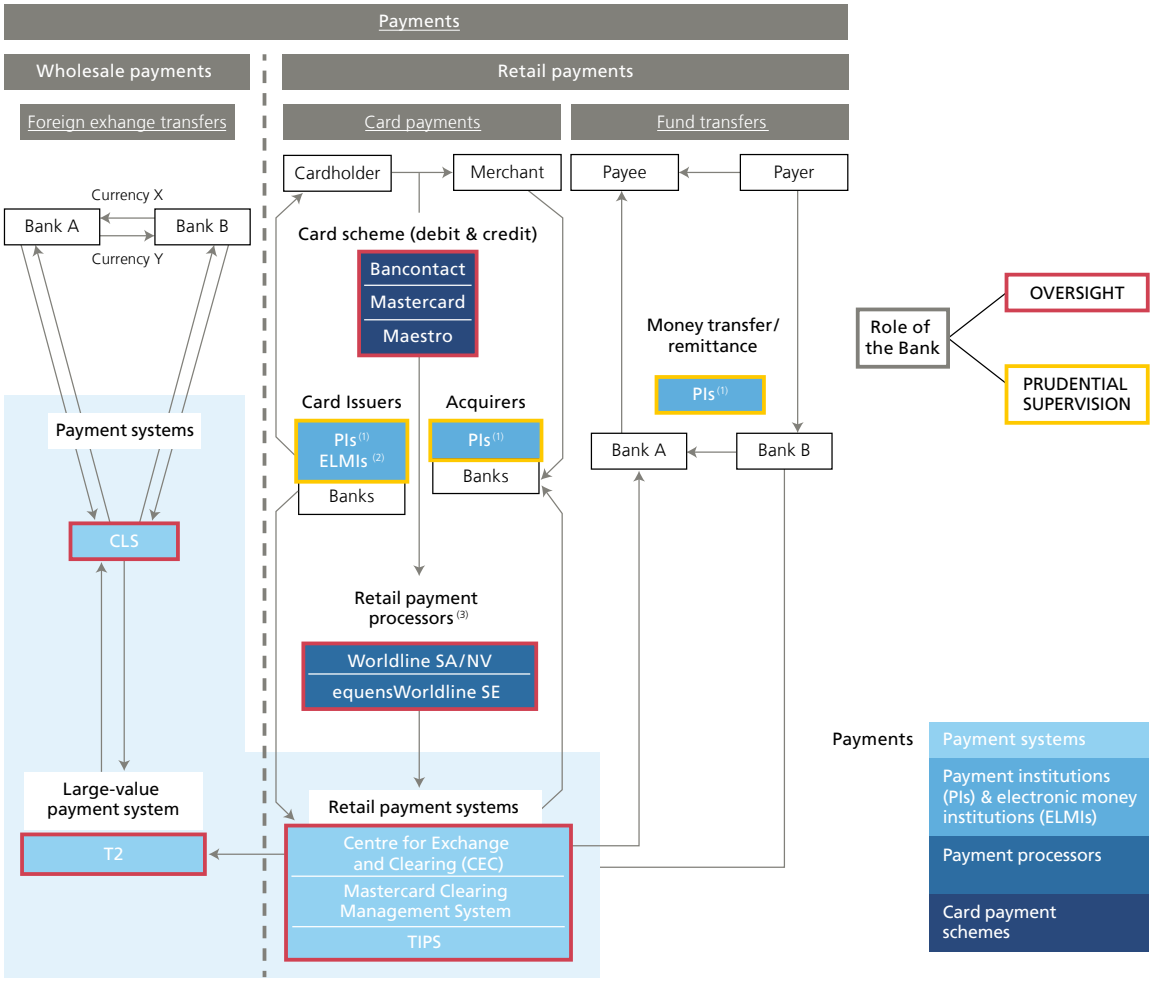
Section 3.4 covers the three payment card schemes overseen by the Bank: the domestic Bancontact scheme and the international Maestro and Mastercard schemes (the latter two are operated by Mastercard Europe SA/NV).

Finally, section 3.5 provides an overview of the digital euro project.

1 The acquisition of card payments is a service whereby a payment service provider enters into a contractual arrangement with a payee (merchant) to accept and process payment transactions guaranteeing the transfer of funds to the latter. The processing is often performed by another entity.

Figure 3

Scope of the Bank's oversight and prudential supervision role in the payments landscape



1 Payment institutions (PIs).
2 Electronic money institutions (ELMIs).
3 Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland Ltd is also designated as a systemic processor for its switching activities for Bancontact according to the Act of 24 March 2017 on the oversight of payment processors but is not overseen by the NBB.

3.1 Payment systems

Changes in the regulatory framework

There were no changes to the Belgian and Eurosystem regulatory frameworks in 2023..

Prudential and oversight approach

Since May 2020, the Mastercard Clearing Management System (MCMS) operated by Mastercard Europe (MCE), established in Belgium, has been designated a systemically important payment system (SIPS) with pan-European reach, based on a number of mainly quantitative criteria, listed in the SIPS Regulation itself. As such, MCMS is subject to joint lead oversight by the ECB and the Bank.

In the course of 2022, the Bank and the ECB, with the support of a Joint Oversight Team (made up of representatives of the Eurosystem NCBs), carried out an official Eurosystem assessment of compliance by the MCMS with the SIPS Regulation, based on analysis of a self-assessment provided by MCMS along with underlying evidence and complemented by numerous exchanges between MCE and the oversight authorities.

The key oversight activities in 2023 were: (1) finalisation of the comprehensive assessment of compliance by the MCMS with the SIPS Regulation, including a fact check by MCE and formal adoption of the report by the Eurosystem governing bodies, as well as provision by MCE of an action plan for implementation of the Eurosystem recommendations; (2) a Cyber Resilience Oversight Expectations (CROE)[1] assessment of MCE (based on a self-assessment) by a joint assessment team coordinated by the Bank and the ECB and made up of participating Eurosystem NCBs; and (3) the monitoring of other actions planned to further improve the cyber resilience of the institution.

The related primary oversight priorities for 2024 include: (1) monitoring of the implementation by MCE of its action plan and (2) finalisation of the CROE assessment (presumably by the end of Q2).

The CEC is the domestic retail payment system which processes most interbank retail payments in Belgium (i.e. those for which the payer and payee have accounts held with different Belgian banks). These payments include SEPA credit transfers (SCTs), SEPA direct debits (SDDs),[2] card payments, legacy cheques and, on a dedicated platform launched in 2018, instant payments. The Bank is responsible for oversight of the CEC, which is done in the Eurosystem context on the basis of the Revised Oversight Framework for Retail Payment Systems.[3] The latter is itself based on the PFMI. The CEC, which qualifies as a prominently important retail payment system (PIRPS), is compliant with the applicable standards.

In 2023, the CEC focused on preparations for changes to be implemented in 2024 in view of the adoption of the Instant Payments Regulation: these included the IBAN name check and the wider mandatory use of instant payments. During this preparatory period, no major changes were made to the system, while the Bank's oversight work consisted primarily of monitoring.

1 The CROE are based on the Guidance on cyber resilience for FMIs, published by the CPMI-IOSCO in June 2016. The Cyber Resilience Oversight Expectations themselves aim to provide overseers with a clear framework to assess the cyber resilience of systems and enable FMIs to enhance their cyber resilience. Unlike other sets of oversight standards applicable to payment systems (i.e. the PFMI), the CROE enable overseers to determine for each of eight specific domains which of the three maturity levels (evolving, advancing, innovating) must be achieved by the system according to its risk profile and specific activities. The eight domains covered by the CROE are governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving.

2 SCT and SDD are the pan-European payment instruments schemes for domestic and cross-border credit transfers and direct debits throughout the SEPA zone.

3 See https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf.

3.2 Payment institutions and electronic money institutions

Changes in the regulatory framework

In 2022, the Bank published a uniform letter[1] clarifying the existing rules on the composition of statutory governing bodies and, in 2023, paid special attention to the establishment, alignment and formalisation of proper governance structures within payment and electronic money institutions.

The uniform letter focused on three main points, namely: (1) an institution's board of directors must consist of a majority of non-executive directors; (2) members of the board of directors or the management committee of an institution may not hold any other position as an employee in the same institution and must have self-employed status; and (3) there is a potential incompatibility between membership on the board of directors or management committee and holding an independent control function.

In 2023, the Bank began a cross-cutting analysis of (1) the outsourcing policies of supervised institutions and (2) reporting under the segregation and safeguarding policies of supervised payment and electronic money institutions. Analysis of the latter led the Bank to conclude that insufficient information was available to supervised institutions regarding the expected structure of the reporting or its precise content. Disclosures differed in terms of their format, content and quality, leading to an expansion of, or complicating, off-site prudential analysis. Recent on-site inspections resulted in a series of recommendations regarding the operational functioning of client asset segregation and safeguarding. In order to provide clarity to the sector and improve and strengthen both off-site and on-site prudential activities, a decision was taken to issue a new circular on this subject.[2]

The additional reporting requirements laid out in the new circular concern, among other things: (1) the clear identification of each type of fund held by the institution that is used to protect funds received from payment service users; (2) the management of access to client accounts, (3) the method and procedure used to calculate cash flows in client accounts, investments and guarantees; (4) the escalation procedure in the event anomalous or atypical transactions are detected; (5) the management and reconciliation process between the books of account, on the one hand, and client accounts, on the other; (6) the investment policy when investing in a recognised money market fund and/or in safe, liquid assets with a low degree of risk; (7) the procedure to be followed when the method of protecting funds received by an institution from payment service users proves insufficient to cover the full amount of customer funds at any given time; and (8) the internal control measures taken with regard to the protection of the funds of payment service users.

With regard to the priorities for ongoing prudential supervision, the Bank intends in 2024 to: (1) start a new cross-cutting analysis of reporting for the 2023 financial year, as described in the new circular on segregation and safeguarding,[3] and continue to monitor the segregation and safeguarding requirements of funds received by payment and electronic money institutions from payment service users, both on an off-site and on-site (the safeguarding and segregation obligation is and remains a priority) and (2) compare the results of the cross-cutting analysis of outsourcing policies between institutions of similar size that carry out the same type of activity and report the conclusions to management with a view to drawing up a supervisory action plan for 2025.

1 Uniform letter to all payment institutions, registered payment institutions, e-money institutions and limited e-money institutions dated 8 February 2022.

2 Circular NBB_2022_13 dated 3 May 2022 is replaced by Circular NBB_2023_12 dated 9 January 2024 on the protection of funds for the execution of payment transactions and funds in exchange for electronic money.

3 Circular NBB_2023_12 dated 9 January 2024 on the protection of funds for the execution of payment transactions and funds in exchange for electronic money.

BOX 6

A third payment services directive and a payment services regulation

The revised Payment Services Directive,[1] also known as PSD2, was published in the Official Journal of the EU on 23 December 2015 and has been in force since 13 January 2018. It was transposed into Belgian law in early 2018 by two legislative acts.[2] PSD2 regulates the provision of payment services in the EU and aims, in particular, to improve on the first Payment Services Directive, by focusing on (1) increasing payment security through the adoption of strong customer authentication (SCA) and (2) increasing competition through the creation of a non-contractual right of access to payment accounts ("open banking").

On 28 June 2023, the European Commission submitted a proposal to review PSD2, paving the way for a third Payment Services Directive (PSD3), and a proposal for a Payment Services Regulation (PSR). The purpose of the proposals is to bundle the prudential rules on the status, rights and obligations of payment institutions into a new directive and incorporate the remaining rules, as well as the granting of rights to consumers, merchants and payment service providers, into a directly applicable regulation. The regulation will govern liability when something goes awry in the execution of a payment or in the case of a fraudulent payment. In addition, it is intended to include complementary rules on strong customer authentication and open banking.

The proposal contains a few noteworthy changes to the existing legal framework, mentioned in the following non-exhaustive list:

(1) It aims to combat and mitigate fraudulent payments by seeking to allow payment service providers to exchange more information between themselves in relation to fraudulent payments and to extend the refund right of consumers that fall victim to identity theft (copying the identifying characteristics of a person, brand or organisation for fraudulent purposes) as well as imposing a mandatory IBAN name check for all SEPA credit transfers.
(2) The proposal promotes/facilitates open banking by removing the remaining obstacles to the provision of open banking payment services while increasing the control that payment service users have over their payment data and clarifying previous points of contention.
(3) The proposal strengthens harmonisation and enforcement by crafting rules in a directly applicable regulation and incorporating e-money services into the PSD framework.

The proposal is currently under discussion in the Council and was an important focus area of the legislative work carried out under the Belgian presidency of the Council of the European Union in the first half of 2024.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (hereafter "PSD2").

2 Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions and access to the activity of payment service provider, to the activity of issuing electronic money and to payment systems and the Act of 19 July 2018 amending and introducing provisions on payment services in various books of the Code of Economic Law.

Prudential and oversight approach

Last year, one institution [1] was granted a licence as a Belgian payment institution, while two payment institutions [2] were removed from the official list due to consolidation at group level. In 2023, one account information services provider was added to the official list and one withdrawn, leaving the number at six. The number of electronic money institutions remained unchanged, at five. Consequently, the number of Belgian institutions dropped slightly and stands at 38 compared with 39 the previous year. The tally of European branches present in Belgium increased from eight to ten.[3] Taking Belgian institutions together with European branches, there are 48 institutions, altogether, representing an increase of one institution compared with 2022.

Bancontact Payconiq NV, which previously offered regulated payment services in Belgium under the licence of the Luxembourg payment institution Payconiq International SA, was authorised as a Belgian payment institution by the Bank in February 2023. The company holds a significant share of the Belgian mobile payments market with over 500 000 mobile payment contact points across Belgium and a significant share of the Belgian peer-to-peer mobile payments market. This is in addition to its activities as the operator of the Belgian card payment scheme Bancontact.

A decision from the Belgian government on the mandatory introduction of digital invoicing, or e-invoicing, between companies as from 1 January 2026 could be an opportunity for entrepreneurs from the world of online invoicing platforms and accountants to submit applications for licences to offer account information services.

In 2023, the increase, already observed last year, in the registration of limited network exclusions continued. Indeed, PSD2 introduced an exclusion from its scope of application for services based on specific payment instruments that can only be used in a limited way. Two out of four [4] new registrations pertained to the mobility sector and two to the gift cards sector. One registration, concerning the provision of virtual asset services, was relinquished. At the end of 2023, there were 12 limited network exclusions on the Bank's official list.

As noted in last year's Financial Market Infrastructures Report, the Brexit-related relocation of payment institutions has profoundly changed the Belgian money remittance landscape. A number of money remitters decided to relocate to Belgium, with the result that the volume of transactions processed via Belgian payment institutions rose considerably between 2019 and 2021.

At the end of 2021, the volume of remittances processed by Belgian money remitters (and EEA money remitters active in Belgium) stood at €17 304.8 million, of which 97.1 % was processed via Belgian payment institutions. In 2022, this rose to €19 093 million. The strong increase in the volume of money remittances was mainly driven by the digitalisation of the remittance market.

Given its position as a knowledge centre for money remittances and its public interest tasks, the Bank has been asked to participate in the International Organisation for Migration (IOM) O-REMIT project. Belgium has committed to reducing the cost of money remittances to 3 % per transaction ; a better understanding of diaspora remittances and behaviour in Belgium can shed light on cost-efficient remittance options and help the diaspora in Belgium make meaningful investments in their home countries.

1 Bancontact Payconiq Company SA.
2 Alpha Card CVBA and Alpha Card Merchant Services CVBA.
3 Aera Payment & Identification AS and Brink's Payment Services SAS.
4 DKV Euro Service Gmbh, Telepass S.p.A, Airbnb Ireland UC and Zalando SE.

BOX 7

MICA

In 2023, the EU's new legislative framework for crypto-assets, the Markets in Crypto Assets Regulation (MiCA), entered into force. This regulation forms a key part of the European Commission's digital finance strategy.

MiCA is being implemented within a "crypto ecosystem" which already boasts more than 10 000 projects, with increasing volumes of investment being channelled into both Bitcoin and other, often lesser-known, crypto-assets. However, these assets have not always proved to be successful ventures, as illustrated by the number of bankruptcies (e.g. Celsius Capital, FTX, BlockFi and Three Arrows Capital), scandals (e.g. the Bitfinex exchange hack) and instances of fraud (e.g. pump and dump schemes) that have rocked the ecosystem. Crypto-asset markets also suffer from a lack of transparency (particularly in terms of liquidity and reserves), professionalism, and protection for investors and users.[1] In the meantime, larger and more traditional financial actors are entering the crypto and stablecoin space (e.g. Paypal, Société Générale).

With this in mind, the European Commission's aims for MiCA are manifold, starting with establishing legal certainty for crypto-assets within the European Union. Differences in the treatment of these assets across EU member states and the partial application of pre-existing legislation to the ecosystem require a response commensurate with these challenges. The regulation also seeks to stimulate innovation, while ensuring that consumer protection and market integrity are not undermined. Furthermore, despite crypto-assets not (yet) posing financial stability issues given that their total outstanding value is not considered significant (compared with the market capitalisation of traditional finance), this is a topic under constant regulatory scrutiny worldwide, and MiCA is therefore a welcome step forward.

Three categories of crypto-assets fall under the scope of MiCA, two of which are defined as "stablecoins". Particular attention is given to this form of crypto-currency due to a number of specific concerns. Firstly, stablecoins can potentially be backed by one or more traditional fiat currencies. Secondly, the anxiety engendered by their wider use as a medium of exchange (compared with other crypto-assets) means that they have avoided the volatility experienced by other crypto-currencies such as Bitcoin. Lastly, the risks associated with crypto-currencies in general have compounded the sense of urgency around legislative action. Indeed, once investor confidence in an issuer's liquidity reserves is lost, stablecoins can also lose value at lightning speed (e.g. Terra/Luna).

MiCA addresses these risks by first identifying two types of stablecoins: electronic money tokens (EMTs) and asset-referenced tokens (ARTs). The value of EMTs is determined with reference to the price of an official fiat currency, while the value of ARTs is determined based on the value of several fiat currencies, one or more commodities or crypto-assets, or a combination of such assets (e.g. X8C, which is backed by a basket of eight major currencies and gold). Issuers of these two categories of stablecoins are subject to multiple rules. Key among these is that prior to being allowed to offer such a stablecoin in the EU, the issuer must notify their national competent authority (NCA) through a white paper – subject to NCA approval in the case of an ART – and publish it, thus ensuring transparency and accountability to investors. Other rules relate to investment of the funds received, reserve assets, investor redemption rights, consumer/investor protection, and liability for marketing.

1 For more information, please refer to the joint warning by the FSMA and the Bank on the use of crypto-assets.

The third category of crypto-assets covered by the new regulation includes legacy forms of the "crypto ecosystem" under the term "residual crypto-assets", which corresponds, but is not limited, to Bitcoin, Ether and utility and loyalty tokens, for example. These assets, the value of which does not depend on a reserve asset, will be subject to a "light" regulatory regime (with the exception of those crypto-assets already on the market). This will entail a simple registration requirement with the NCA rather than ex ante notification or approval, the publication of a white paper for which the issuer is legally responsible, and strict conditions regarding marketing to ensure an adequate level of consumer protection.

In addition to seeking to regulate issuers of crypto-assets, MiCA also captures so-called crypto-asset service providers (CASPs) in its scope, given that the European Commission considers these entities to be a gateway to traditional finance. As defined in the regulation, a CASP is a legal entity that provides one or more crypto-asset services[1] in a professional capacity. Along with extension of the existing rules in the payments and securities sector (e.g. outlawing market abuse such as frontrunning) and rules specific to the service provided by each CASP, they will be required to comply with rules related to governance, the prevention of conflicts of interest, outsourcing, and the investment of crypto-assets. It is worth noting that most non-fungible tokens, unlike CASPs, do not fall within the scope of MiCA and will be studied in a more targeted way in the coming years by the European Commission.

The European Supervisory Authorities[2] and the NCAs are responsible for implementing the legislation[3]: the European Banking Authority (EBA) will be in charge of the supervision of significant EMTs and ARTs while the European Securities and Markets Authority (ESMA) will be responsible for providing the Commission with systematic reporting and feedback, establishing and maintaining a register with information on crypto-assets white papers and issuers of EMTs and ARTs, and ensuring coordination and cooperation between NCAs. The latter will in turn be responsible for oversight of non-significant EMTs and ARTs as well as CASPs, with the possibility to suspend their service offering, make public the fact that a CASP is not compliant with regulatory standards, suspend advertising, instruct auditors, impose fines, and ban members of management from holding office. In addition, NCAs will also ensure market surveillance by preventing practices such as market manipulation or insider trading.

MiCA entered into force on 29 June 2023 upon publication in the Official Journal of the European Union, with Titles III and IV (concerning ARTs and EMTs) expected to come into effect in June 2024 and the remaining titles (including those related to crypto-asset service providers) in December 2024.

Implementing legislation in the form of delegated acts is being developed by the EBA. The Bank is playing an active role in this process via participation in technical working groups. This work includes the development of 17 technical standards and guidelines to further specify the requirements for asset-referenced tokens, electronic money tokens and crypto-asset service providers. The authorities have not yet, however, decided on the role or responsibilities that will be allocated to the Bank under this new legal framework.

1 These services include but are not limited to the custody and administration of crypto-assets on behalf of third parties, the operation of a trading platform for crypto-assets, the exchange of crypto-assets, the execution or receipt and transmission of orders for crypto-assets on behalf of third parties, and the provision of advice on crypto-assets.
2 In this case the European Banking Authority and the European Securities and Markets Authority.
3 Partial implementation for all aspects related to EMTs and ARTs is planned for the spring of 2024, with final implementation (including CASPs) in the autumn of 2024.

3.3 Payment transaction processors

Changes to the regulatory framework

The Belgian regulatory framework applicable to payment transaction processors remained unchanged in 2023.

Prudential and oversight approach

According to the Act of 24 March 2017 on the oversight of payment processors, systemically important processors must comply with requirements that aim to maintain the stability and continuity of retail payments in Belgium, e.g. compulsory, comprehensive risk management in the fields of detection, appraisal and the development of mitigation measures. The legal framework for payment processors also includes a strict process for the reporting of incidents to the Bank and enables the latter to apply a sanctions regime.

In 2023, no new entity was notified as a systemically important payment processor. A list of entities with this status under Article 6 of the abovementioned act and the scheme(s) to which this status applies is available on the Bank's website.[1]

3.4 Card payment schemes (CPS)

Changes to the regulatory framework

No changes were made in 2023 to the Belgian and Eurosystem regulatory frameworks applicable to card payment schemes. These were fully reviewed in 2022, upon the adoption by the Eurosystem of a new oversight framework for electronic payment instruments, schemes and arrangements (the PISA framework).

Prudential and oversight approach

The Belgian CPS, Bancontact, is subject to oversight by the Bank. In 2023, it was assessed against the PISA framework, on the basis of a self-assessment reviewed by the Bank, which is responsible for evaluating compliance with PISA. Prior to finalisation, the assessment report was submitted to other Eurosystem central banks for peer review. The assessment process did not identify any violation of the oversight principles.

For MCE, which qualifies as both a CPS and a SIPS, the PISA framework provides – with a view to avoiding overlapping tasks – for account to be taken of the results of all prior oversight exercises to monitor its compliance (see section 3.1) with the requirements of the SIPS Regulation.

A review was carried out in 2022 to determine the parts of the PISA framework assessment methodology that had not yet been addressed by the comprehensive assessment of MCE's compliance with the SIPS Regulation. Due to a delay in the CROE assessment, the assessment of MCE's compliance (as a CPS) with the PISA framework began in April 2024.

1 See https://www.nbb.be/en/financial-oversight/oversight/payment-systems-card-schemes-and-processors-payment-operations-2.

3.5 Digital euro project

For the past few years, the Bank and the Eurosystem have been investigating – in collaboration with market stakeholders including consumer representatives, academics, and members of the National Retail Payments Committee (at Belgian level) – the possible creation of a digital euro. The digital euro would be designed to cover all retail payment scenarios, providing users with the possibility to carry out simple transactions instantly and free of charge, online and offline, in the euro area. The creation of a new unit within the Bank, the Digital Euro and Payments Policy Unit, underscores the growing importance of this project to modernise the European retail payments landscape.

The Eurosystem's efforts, along with the results of various consultations, have meant that progress has been made on the potential design of a digital euro. As such, on 18 October 2023, the ECB's Governing Council decided to move to the preparatory phase of the project. This section revisits the reasons leading to this decision before delving deeper into the design and features of the digital euro[1] and setting out the next steps in the project.

A project guided by the times...

The journey towards a digital euro is being driven not only by technological innovation but also by the changing nature of modern society. This project is a strategic step towards increasing Europe's autonomy and resilience in the digital financial landscape: a digital euro would ensure a public means of payment developed under pan-European governance and standards, which would be particularly important in times of crisis or geopolitical tensions.

In addition, developments such as the metaverse and artificial intelligence signal a major shift towards the digital realm. The EU's common currency must be ready to cope with this transition. This project represents the Eurosystem's unwavering commitment to ensuring that money continues to evolve in tandem with the needs of society and includes enabling machine-to-machine transactions in the fourth industrial revolution ("Industry 4.0") and facilitating conditional payments in the evolving landscape of Web 3.0.

To support this forward-looking vision, European lawmakers have taken decisive steps. The European Commission launched the legislative process for a digital euro with the release of its Single Currency Package in June 2023.[2] This proposal is currently being considered by the European Parliament and the Council. It effectively recognises that in a society embracing digitalisation, it is important to adapt the key features of physical cash – such as confidentiality, offline usability, resilience, mandatory acceptance, and a distinct European brand – to the digital realm. Importantly, the European Commission, like the ECB, has made its objective clear: the digital euro is not intended to replace physical cash but rather to serve as an additional option for consumers and merchants, regardless of the time and place of a transaction. The European Commission has therefore included a provision on the legal tender status of cash in its legislative proposal, in order to preserve and protect the role of cash in our society.

... and by society as a whole

It is important to stress that, in this context, the abovementioned actors are not the only driving force behind this initiative. The common currency of the EU and its form – whether physical or digital – affect the lives of all citizens, beyond the specific concerns of central bankers and policymakers. Consequently, public consultation cycles, discussion groups, advisory committees, regular bilateral meetings and conferences have been or are being organised. The aim of these initiatives is to achieve the widest possible diffusion of the project, thereby ensuring inclusive and representative participation from society at large.

1 Subject to the work carried out by the European Commission, Council and Parliament.
2 See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3501.

Key features of the digital euro

The digital euro would be a versatile currency, accessible online and offline and covering all (basic) retail payment use cases, instantly and free of charge, throughout the euro area. It could be used for person-to-person (P2P) transactions as well as in e-commerce and point-of-sale (POS) situations, enabling public money[1] payments for both in-store purchases and online shopping. The digital euro could also help to streamline government-to-individual or government-to-business (G2X) transactions, such as the disbursement of benefits or subsidies.

It would be possible to access the digital euro using everyday banking applications as well as a standalone application provided by the Eurosystem. However, there would be limits on the volume of funds that could be uploaded to a digital euro account. In addition, the Eurosystem aims to provide several defunding and funding options, including the automatic defunding of a digital euro account triggered by an incoming payment that would result in the user's digital euro position exceeding the individual holding limit (known as the "waterfall functionality") and the automatic funding of a digital euro account triggered by an outgoing payment that exceeds the amount held in the user's digital euro account (the "reverse waterfall functionality"). These options, including manual and automatic (de)funding, would be designed to ensure that the holding limit does not become a transaction limit, thereby enabling consumers to use the digital euro as a medium of exchange while preventing its use as a store of value.

To enhance payment flexibility, transactions could be executed through smartphones or physical payment cards. The possibility of using near field communication (NFC) and quick response (QR) codes to facilitate payments is being examined. In addition, the digital euro should enable users to establish conditional payments, thereby streamlining transactions when predetermined criteria are met. This functionality could prove particularly beneficial for payment service providers (PSPs) seeking to innovate and create specialised services utilising the robust infrastructure of the digital euro.

From the investigation phase to the preparation phase

Work on a digital euro started in October 2020, when the ECB published a report on its feasibility.[2] A public consultation on the benefits and challenges of issuing a digital euro and its possible design was then conducted from October 2020 to January 2021.

The investigation phase, which focused on key issues relating to the design and distribution of the proposed new digital currency, began in July 2021 and ended on 18 October 2023, at which time the ECB Governing Council decided to proceed to the preparatory phase. This new phase, which will last at least two years, aims to finalise the rules necessary for the creation of a digital currency. It is also intended to allow more in-depth analysis of the various components of the platform that will need to be set up for tendered services, as well as of the private and public entities responsible for providing these services.

As this work progresses, clear and accurate communication will be crucial to shaping public understanding and building trust in the digital euro project. To counter misinformation, the Bank is committed to ensuring transparent communication, as reflected in this new section of the FMI Report.

The Bank held a conference entitled "A Digital Euro for the Digital Era" on 7 September 2023.[3] The line-up of speakers, which included representatives of central banks, European institutions, the payments industry and consumer associations, ensured that the views of a wide range of stakeholders were shared.

1 Public money is issued by central banks, while private money is issued by commercial banks.
2 See https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.
3 See https://www.nbb.be/fr/events/digital-euro-digital-era-video.

Conclusion

The potential issuance of a digital euro[1] signals the Eurosystem's firm commitment to ensuring that money – as it has always done throughout history – continues to evolve in step with the society it serves. This commitment entails two fundamental objectives: preserving continued access to physical cash in our societies and maintaining the relevance and utility of public money in the digital era. To achieve these objectives, it is imperative that the digital euro seamlessly integrate the core attributes of the physical euro into the digital realm. These attributes include confidentiality, offline usability, resilience, mandatory acceptance and a distinct European branding. At the same time, it should remain adaptable to future payment requirements, such as facilitating machine-to-machine transactions in Industry 4.0 and enabling conditional payments in the decentralised landscape of Web 3.0.

The aim of the digital euro is thus not to replace cash, but rather to serve as a continuously available payment option for consumers and merchants, regardless of where and when a transaction takes place.

1 Falling under the authority of the ECB Governing Council and subject to a proportionality assessment at the end of the legislative process.

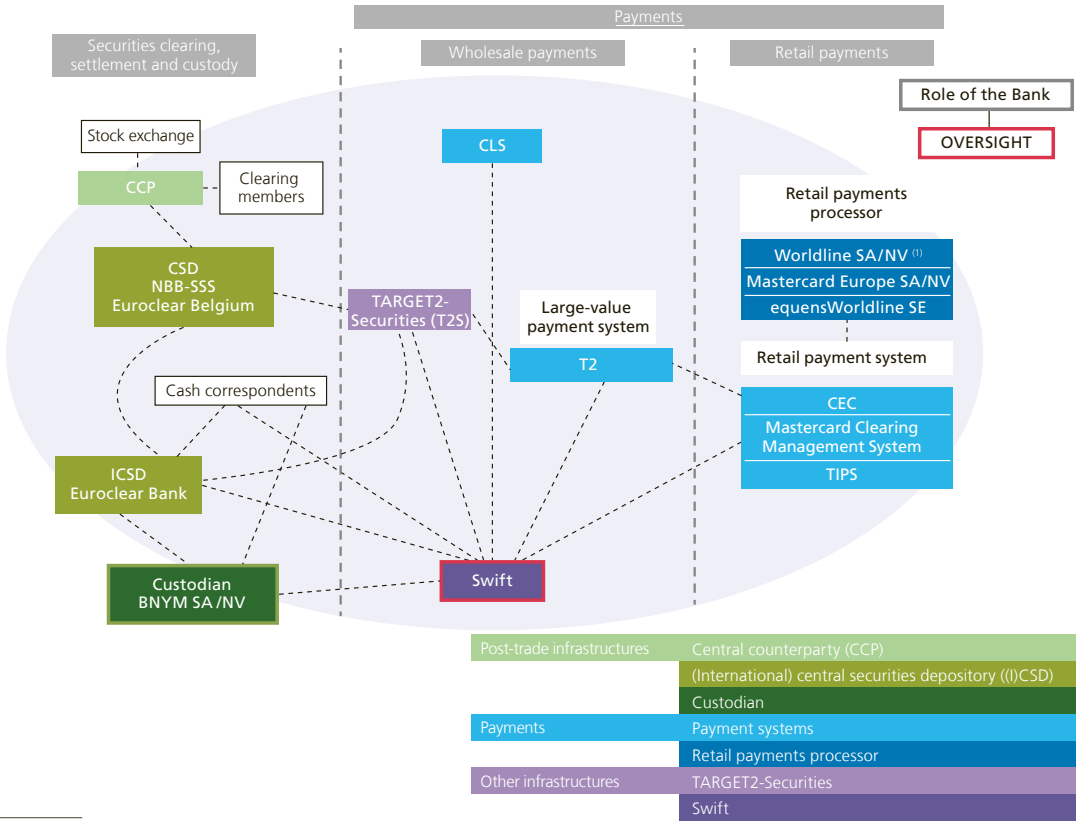
4. Swift

The Society for Worldwide Interbank Financial Telecommunication (Swift) is a limited-liability cooperative company that provides messaging services to financial institutions and market infrastructures across the globe. Swift serves different types of customers, which vary in terms of their size and activity, including banks, brokers, investment managers, fund administrators, custodians, corporates and Treasury counterparties. Swift is registered in Belgium, with its headquarters in La Hulpe.

Through its financial messaging services, Swift plays a crucial role in facilitating correspondent banking and financial market infrastructure operations. This fundamental role in the global financial sector creates significant systemic dependency on Swift. Hence, the G10 established a cooperative oversight framework to monitor Swift's activities with the aim of safeguarding financial stability.

Figure 4

Swift as a critical service provider to the financial industry



1 Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland Ltd is also designated as a systemic processor for its switching activities for Bancontact according to the Act of 24 March 2017 on the oversight of payment processors but is not overseen by the NBB.

4.1 Swift oversight framework

4.1.1 Swift and its users

As a member-owned cooperative, Swift is owned and controlled by its users. To facilitate engagement and involvement, Swift's users are organised into National Member Groups. National Member Groups comprise all Swift shareholders in a country and propose candidates for election to Swift's board of directors. They act in an advisory capacity to the board of directors and Swift's management. The composition of Swift's board is designed to reflect the use of Swift messaging services, ensure its global relevance, support its international reach, and uphold its strict neutrality. A nation's use of Swift's messaging services determines both its Swift shareholding allocations and the number of board members to which it is entitled. Shares are reallocated based on the financial contribution of shareholders for network-based services. Since this factor varies over time, the shares are reallocated every three years to mirror actual usage of Swift messaging services. The next reallocation is scheduled to take place in 2024.

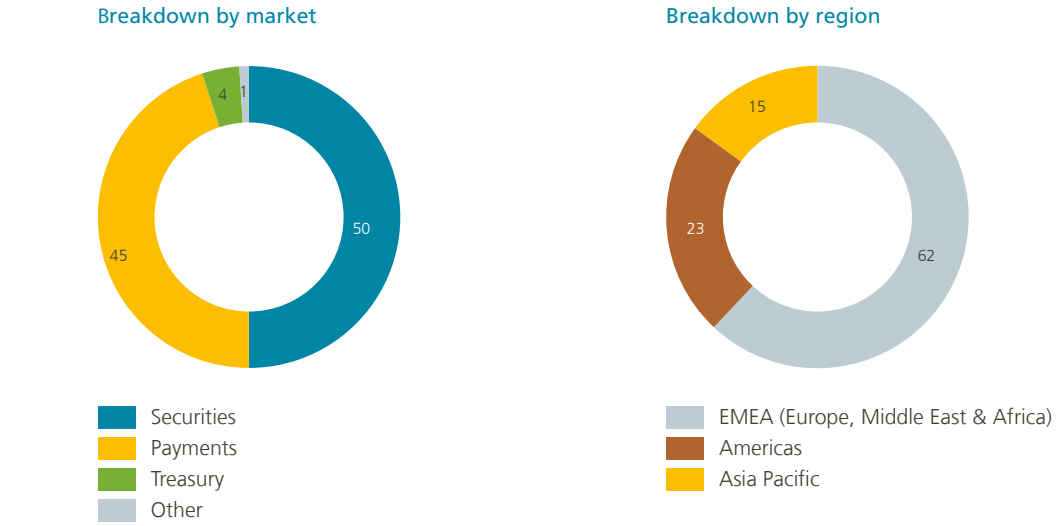
The following numbers reflect Swift's global reach and its important role in the global financial infrastructure. Swift provides messaging services to customers located in more than 200 countries, amounting to approximately 11 800 registered live users, of which 2 335 are Swift shareholders. In 2023, 11.9 billion messages were sent with a daily average of 47.6 million.

The core service for the exchange of financial messages is Swift's FIN application. The following figure shows FIN traffic for 2023 distributed by region and market, respectively. In line with figures for previous years, the payments (45 %) and securities (50 %) markets represented the lion's share of Swift's messaging traffic volumes in 2023. The Europe, Middle East and Africa (EMEA) region accounted for the largest share of total 2023 FIN traffic volume, followed by the Americas and the Asia Pacific region. It should be noted that the migration to ISO 20022 led to a revision of the calculation method for these results, resulting in FIN InterAct Payment flows being included in the payment metrics as from March 2023. Please see section 2.3 below for more information on the migration to ISO 20022.

Figure 5

Swift FIN traffic distribution by region and market

(2023)



Source: Swift.

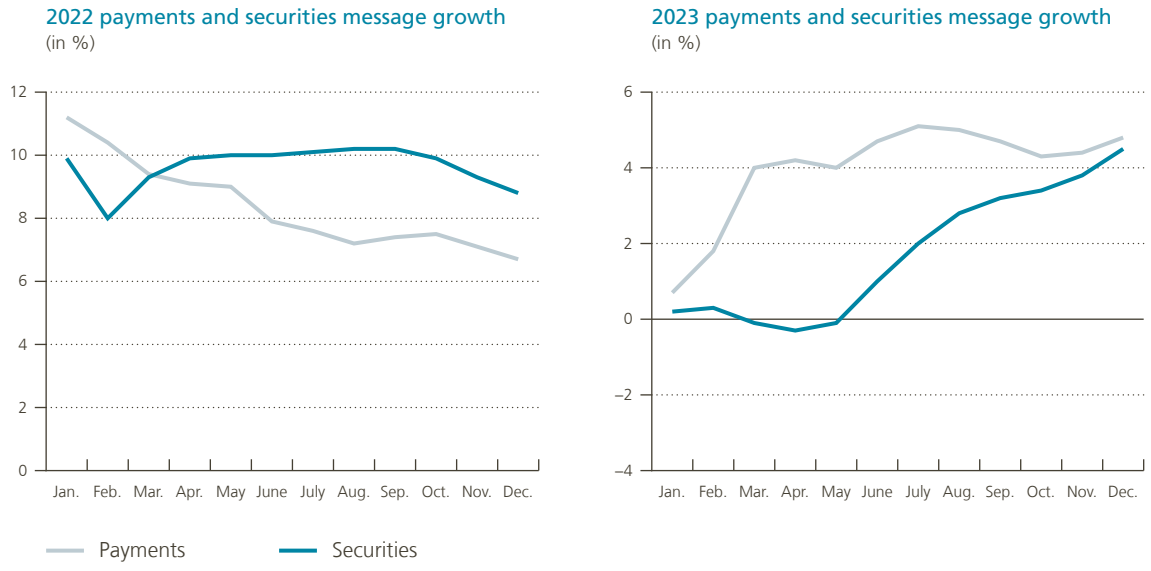
In 2023, despite numerous continuous challenges, such as a global economic slowdown, persistent inflation, turmoil on the financial markets and geopolitical instability, Swift reported positive growth in messaging traffic related to both payments (4.8 %) and securities (4.5 %) at year's end. These figures contributed to overall FIN traffic growth of 4.5 % for 2023.

The mild growth in securities traffic in 2023 (+4.5 %) was due to a slowdown in the first half of the year, attributed to reduced volatility and investment activity. On the other hand, the growth in payments in 2023 (+4.8 %) was on par with 2022, owing to sustained instruction volumes growth alongside test volumes for ISO 20022 migration. This was partly offset by a slowdown in reporting flows compared with historical averages.

The following two graphs show the percentage change in FIN payments and securities traffic for 2022 and 2023, respectively.

Figure 6

Growth in payments and securities messaging traffic in 2022 and 2023



Source: Swift.

4.1.2 International cooperative arrangement

In 1997, the G10 central banks[1] formalised the Swift oversight arrangement for the purpose of monitoring the adequate and safe functioning of this critical service provider. In addition to the participating G10 countries, the Bank for International Settlements and the European Central Bank are represented in the international working groups. As Swift is headquartered in Belgium, the Bank acts as lead overseer and chairs the international oversight meetings.

The G10 central banks are represented in four working groups: the Technical Group (TG), which conducts technical fieldwork; the Cooperative Oversight Group (OG), the decision-making body which sets oversight strategy; the Executive Group (EG), which serves as the interface for overseers to communicate conclusions and

1 The G10 central banks involved in Swift oversight are the Bank of Canada, the Deutsche Bundesbank, the European Central Bank, the Banque de France, the Banca d'Italia, the Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, the Swiss National Bank, the Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

recommendations to Swift's board and executive management; and the Oversight Forum (SOF), which brings together a wider group of central banks to discuss oversight activities and relevant changes at Swift.

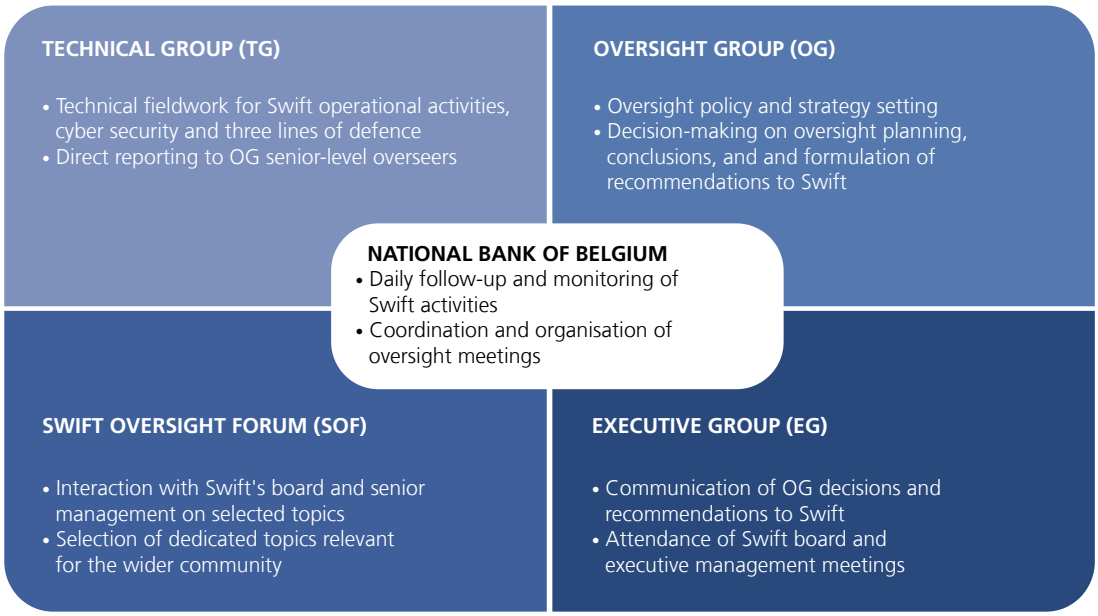
Given the systemic nature of Swift, a larger group of G20 countries are directly involved in oversight. These G20 central banks are represented in the SOF. Membership corresponds to their share of total Swift traffic volume and the CPMI membership composition. The SOF deals with Swift oversight conclusions, planning and priorities, the Customer Security Programme, and other specific topics. In-person meetings of the SOF will resume in 2024, following a temporary switch to virtual meetings to comply with statutory and regulatory public health requirements during the Covid-19 pandemic.

In its capacity as Swift's lead overseer, the Bank has a dedicated team which conducts daily monitoring and follow-up of Swift's activities and projects. As formulated in the Swift Oversight Protocol, the Bank serves as the entry point for channelling information to the other overseers and, as chair, coordinates the various working groups in terms of reporting to the other overseers and preparing discussion items.

More information on the composition and activities of each working group, as defined in the current oversight framework, can be found in previous editions of this report (2017–2023). The figure below provides an overview of the working groups involved in the oversight of Swift.

Figure 7

Swift oversight working groups involving G10 and G20 central banks



Source: Swift.

Oversight of Swift is based on five High-Level Expectations (HLEs), i.e. (1) Risk Identification and Management, (2) Information Security, (3) Reliability and Resilience, (4) Technology Planning, and (5) Communication with Users. These five HLEs are set out in Annex F to the CPMI-IOSCO's Principles for FMIs and form the oversight expectations applicable to all FMI critical service providers.

The activities of overseers are anchored in the five HLEs which drive their planning and priorities. Overseers assess the adequacy of Swift's management of operational and security risks across the three lines of defence, comparing it with these expectations. Swift is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. the provision of required documentation, interaction with Swift's three lines of defence, and discussions with executive management and the board).

More information on how the oversight activities for 2023 can be linked to each of the five HLEs can be found at the end of this section.

4.1.3 Changes to the Swift oversight arrangement

The Oversight Group (OG) is currently revising the oversight framework set out above. The current framework is based on a memorandum of understanding (MoU) concluded between Swift and the Bank, as well as additional MoUs concluded by the Bank with each G10 central bank directly involved in the oversight of Swift, including the European Central Bank. As mentioned above, the Bank has been designated the lead overseer of Swift.

The current oversight framework focuses primarily on various operational risks. As stated above, overseers have translated these operational risks into five High-Level Expectations (HLEs). Two HLEs focus on risk management (HLE 1, Risk Identification and Management, and HLE 5, Communication with Users) while three HLEs deal with the specific types of risks to be managed (HLE 2, Information Security; HLE 3, Reliability and Resilience; HLE 4, Technology Planning).

The use of HLEs provides Swift and its overseers with a common language and a framework within which discussions can be held and overseers can organise their activities. However, oversight discussions are not necessarily limited to topics included in the HLEs, as the oversight framework is broader and can encompass other specific topics for review and discussion with Swift's management and internal audit service.

The last major review of the oversight arrangement dates from 2005. Since then, the regulatory expectations of banking and financial market infrastructure overseers have evolved. For example, Basel III introduced new capital requirements for the banking sector, while the CPMI-IOSCO Guidance on cyber resilience, the Eurosystem's Cyber resilience oversight expectations for financial market participants and Regulation (EU) 2022/2554 on digital operational resilience (DORA) have resulted in changes to expectations with regard to operational risks.

Although these regulations and guidance are not directly applicable to Swift as it is neither a bank nor a financial market infrastructure, Swift's top-tier overseers are of the view that several of these expectations should be codified so as to function as a legal backstop and ensure a level playing field for oversight and supervision of the financial sector. The proposed review of the oversight framework focuses on the importance of Swift as a critical provider of messaging services to the financial sector and recommends aligning the expectations of overseers with customary expectations in the broader financial sector, such as the CPMI-IOSCO Principles for financial market infrastructures (PFMI), whilst taking into account the specific nature of Swift.

The intention of overseers is not to change the content or objectives of the current oversight framework fundamentally, but rather to codify particular aspects of this framework so that it can serve as a legal backstop.

The current organisation of and approach to Swift oversight will be maintained, including the two-tier structure with a technical (TG) and senior-level (OG) oversight body. The revised approach will also seek to maintain collaborative, consensus-building interaction amongst overseers at both the technical and senior levels.

As Swift is a cooperative company under Belgian law, a legislative proposal to be brought before the federal Parliament will be developed, after a consensus is reached on its content within the Oversight Group.

4.2 Selection of major topics analysed by overseers in 2023

A non-exhaustive selection of major topics which overseers analysed in 2023 is presented below. The highlighted topics are not a full representation of the review work conducted in 2023 (e.g. standing topics such as business continuity exercises, effectiveness of the three lines of defence, enterprise risk management and internal audit activities).

4.2.1 Cyber- and physical security

In 2023, oversight work continued to be carried out against the backdrop of the high geopolitical uncertainty that first arose in 2022. As Swift is essentially an ICT company, cyber and physical security is a major focus area for overseers.

Cybersecurity is a broad term that encompasses various fields, each of which focuses on specific aspects of digital security. Managing these fields is crucial to ensuring both security and operational resilience, as they collectively contribute to protecting Swift's information, systems and networks against cyber threats. The areas covered include governance and risk management, identity and access management, application security, data security, incident and response management, and cloud security. Due to their importance and contribution to Swift's overall security posture, these are standing items on the oversight agenda.

One emerging issue in the area of cybersecurity is quantum cryptography, or the leveraging of principles of quantum mechanics to perform cryptographic tasks, such as data encryption, and ensure the security of communication channels.

From an oversight perspective, monitoring the development of Swift's quantum cryptography capabilities is aligned with the objectives of long-term security planning and maintaining data confidentiality, so as to future-proof the environment in which Swift operates and ultimately ensure trust in the global financial sector.

Another topic that attracted the attention of overseers was third-party risk management (TPRM), sometimes referred to as "supply chain risk management" or "vendor risk management". This was covered in depth by way of an on-site review (OSR) in 2023. For more information on the context and outcome of the OSR, please see Box 8.

Physical security is a critical part of an organisation's overall security posture and, in conjunction with cybersecurity measures, helps provide a comprehensive defence against various threats. While cybersecurity focuses on protecting digital assets and information, physical security addresses the safeguarding of tangible assets, facilities and personnel. Accordingly, topics such as asset protection and the physical security of Swift's data centres and operating locations, the prevention of unauthorised access, business continuity, and resilience and disaster recovery are recurring items on the oversight agenda.

Overseers can organise on-site visits to Swift's offices and locations to further assess its compliance with their expectations in terms of cyber and physical security. Such visits allow overseers to gain insight into the company's operations, including its organisational culture, compliance with technical and security controls, and overall security posture.

BOX 8

On-site review of third-party risk management

The Oversight Group (OG) decided to conduct an on-site review (OSR) in 2023 on the topic of third-party risk management (TPRM) to examine Swift's TPRM practices, policies and procedures and assess whether they adequately meet oversight expectations. Third-party risks refer to those that arise from the use of third-party vendors, suppliers or service providers. These risks can be grouped into several categories, including financial risks, operational risks, cybersecurity risks, business continuity risks and reputational risks.

An example of cyber risk is a supply chain attack. This is an attack on an organisation's suppliers in order to gain unauthorised access to its systems or data. The damage from such an attack can be substantial. Supply chain attacks can be carried out through, among other means, compromising software patches or updates, undermining code signing or manipulated open-source code. A disproportionate reliance on start-up suppliers can also pose a risk as the business model and security practices of newly established companies have yet to prove their effectiveness over time.

The Covid-19 pandemic exacerbated the operational risks faced by financial institutions in relation to the rapid adoption of, and increased dependency on, ICT infrastructure and the sector's growing reliance on technology-based services provided by third parties, of which cloud service providers are a prime example.

The Bank for International Settlements therefore noted that attention should be paid to the appropriate management of third- and fourth-party relationships and concentration risk exposures so as to enhance the ability of financial institutions to withstand, adapt to and recover from potential hazards and mitigate potentially severe disruptive events.[1]

In addition, in this context, the EU took steps to codify certain expectations with regard to third- party risk management in regulations such as the Digital Operational Resilience Act (DORA).

Swift is in the process of updating its vendor risk management processes and practices to keep pace with these developments. Overseers wish to learn more about the actions proposed by Swift to improve its processes and practices. More specifically, they are interested in how Swift currently approaches issues such as the management of third parties, vendor lifecycle management, vendor categorisation, the mitigation of third-party risks, and business continuity as well as changes planned for the future. Against this backdrop, third-party risk management was selected as the focus area for the 2023 on-site review.

In preparation for the on-site review, overseers examined numerous practices and guidelines relating to third-party risk management. Documents provided by Swift were also reviewed to gain insight into existing policies and practices.

The on-site review was carried out over the course of one week, with support from a number of representatives of other central banks. As third-party risk management is a very broad topic, it was

1 See https://www.bis.org/publ/bcbs_nl28.htm.

necessary to interview various people at Swift from different departments, either in-person at Swift's headquarters or virtually, for functions based abroad.

Following the on-site review and taking into account the documents provided and information gleaned from the interviews, the OSR team formulated a number of observations on areas in which improvements could be made. These observations were compiled in a report which was approved by the OG and provided to Swift. Follow-up of the actions undertaken to address these observations will form part of the oversight work carried out in 2024.

4.2.2 Customer Security Programme

Swift's Customer Security Programme (CSP) has been a recurring topic on the agenda of overseers since its introduction following the 2016 Bangladesh bank heist. Swift has created an extensive programme to enhance the cybersecurity of users, their counterparts and the community as a whole. Through the CSP, users are required to adhere to certain controls and good practices to secure appropriately their on-site ICT environments connected to the Swift network. With cyber-attacks on the rise in the financial sector, overseers seek reasonable assurance as to the effectiveness of the CSP and corresponding initiatives designed to adapt to new threats, improve cybersecurity capabilities and adhere to regulatory expectations.

Over the years, Swift has taken multiple initiatives and improved various aspects of its CSP, such as an annual review of its Customer Security Control Framework (CSCF), improvements to the know-your-customer (KYC) tool, the launch of an Independent Assessment Framework (IAF), the introduction of compulsory assessments, more effective involvement of supervisors, actionable updates to the Information Sharing and Analysis Centre (ISAC), and the organisation of recurring awareness campaigns. Thanks to these actions, Swift informed overseers that there has been a downward trend in customer incidents. In fact, since the beginning of 2021, not a single customer incident involving the transmission of a fraudulent message over the Swift network has been reported. Due to the programme's successful track record and promising results, Swift is expected to continue enhancing it.

One expectation concerns the involvement of supervisory authorities in the use of CSCF self-attestation data from financial institutions. From the outset, overseers have encouraged Swift's move to engage supervisors more directly in making effective use of its users' rich self-attestation data, which could provide crucial input for supervisors' risk-based planning and scoping. However, the identification and onboarding of the relevant supervisory authorities in the know-your-supervisor (KYS) tool have proven challenging as, in some cases, multiple supervisory authorities are responsible for a single country. According to Swift's initial reporting to overseers, the use of self-attestation data by onboarded supervisory authorities for financial institutions within their relevant jurisdictions has fallen short of expectations. Overseers have stressed the importance of this initiative and will continue to monitor the actions taken to improve supervisory onboarding and safeguard the effectiveness of the KYS application.

As per standard procedure, overseers contributed, together with the National Member Groups, to the annual review of the Swift Customer Security Control Framework (CSCFv2024), which resulted in one advisory control being made mandatory as well as a number of other changes to the framework:

i. Raising of control 2.8 (Outsourced Critical Activity Protection) from advisory to mandatory to support the ramp-up of outsourcing and use of cloud computing in the community.

ii. Changes to control 2.4A (Back Office Data Flow Security) as well as clarifications and cosmetic changes to improve usability and the implementation of controls.

Swift users are expected to comply with the mandatory controls (i.e. the security baseline) and can certify their compliance with the advisory controls (i.e. good practices for securing local ICT infrastructure) by uploading an attestation (i.e. regarding compliance with the CSCF security controls) using the Know-Your-Customer Self-Attestation (KYC-SA) tool. A new version of the CSCF (v2024) was introduced in mid-2023. Users have until the end of 2024 to submit their attestations.

As of 31 December 2023, 86 % of Swift customers had provided a valid CSP attestation, with 84 % indicating compliance with all mandatory controls. The compliance levels and the number of self-attestations are in line with the uptake in 2021 and 2022. Through Swift's quality assurance and monthly metrics reports, overseers closely monitor various CSP-related variables, such as user attestation and consultation levels. Reporting on CSP metrics is crucial for overseers to obtain a view of the cybersecurity stance of the Swift user community. As such, overseers expect Swift to refine and extend CSP reporting metrics as appropriate.

The Independent Assessment Framework (IAF), which was launched in mid-2021, requires all Swift users to perform a Community Standard Assessment to further enhance the accuracy of their attestations. Every Swift user must have their attestations independently assessed by either an internal independent assessor (e.g. the second or third line of defence) or an external independent assessor (such as a consultancy firm). Users are free to select the internal and/or external resources to be used to conduct this assessment. If a user opts for self-attestation without an independent internal or external assessment, they will be considered non-compliant with the CSP.

Initial reporting on the IAF is in line with that of previous years, with 93 % of users opting for an independent assessor and thus compliant with CSP requirements. Of these users, about half opted for independent internal assessment and half for independent external assessment. The percentage of Swift traffic sent by BICs that provide attestations supported by an independent internal or external assessment is fairly stable at 99 %.

A new addition to the CSP framework was Customer Security Programme Assessor Certification (CSPAC). Swift launched this programme in mid-2023 to address a number of challenges faced by the community in adhering to the IAF, such as scope creep and cost overrun, and in response to requests by customers for a trusted list of certified assessors. These issues were primarily due to gaps in the standardisation of deliverables and inconsistent quality in terms of assessor activity. By means of the CSPAC, Swift aims to raise the expertise of independent assessors, standardise the CSP assessment methodology, and formalise the key outcomes of an independent CSP assessment.

Overseers also assessed Swift's processes for communication with its users on the use of new technologies, incidents of fraud and common cybersecurity threats affecting the community. Swift's Information Sharing and Analysis Centre (ISAC) provides users with actionable information on cyber threats, indicators of compromise and common hacking practices. For example, through the ISAC, Swift shared relevant information on the Log4j vulnerability and the actions its users should take. The timeliness and comprehensiveness of the information shared on such events are also covered by the overseers' review.

4.2.3 ISO 20022 migration and transaction manager

In 2023, the financial sector started migrating to ISO 20022, an open global standard for transferring financial messages and information. The new standard provides consistent, rich and structured data that can be used for all kinds of financial transactions. The migration of Swift's user community to this new standard began over the

weekend of 18-19 March 2023, when cross-border payments and reporting (CBPR+) traffic and a number of market infrastructures, including the Eurosystem's T2 Real-Time Gross Settlement (RTGS) system, EBA Clearing's EURO1 high-value payment system, Australia's Reserve Bank Information and Transfer System (RITS), New Zealand's Exchange Settlement Account System (ESAS), and Canada's Lynx high-value payment system were successfully migrated. In June 2023, the UK's CHAPS and the Bank of England's RTGS system followed suit.

Other market infrastructures, such as the Clearing House Interbank Payments System (CHIPS) and Fedwire, the funds transfer system operated by the US Federal Reserve Banks, will migrate at a later date.

To facilitate the further rollout of ISO 20022 across institutions and jurisdictions worldwide, Swift allows for a co-existence period. This period, during which users are expected to switch from the legacy FIN MT format to the new ISO 20022 MX format, started in March 2023 and is scheduled to end in November 2025. At the end of the third quarter of 2023, ISO 20022 migration for CBPR+ represented around 16 % of total traffic volumes since the start of the coexistence period. Combined with Swift Payments Market Infrastructure (PMI) traffic, the total percentage of payments traffic in ISO 20022 represents 35 %.

As a global standard setter, Swift takes the lead in coordinating ISO 20022 migration for its community. Since the start of this project, overseers have closely monitored Swift's approach, project management and planning, risk assessment and communication with users. They will continue to follow up on Swift's initiatives to facilitate timely migration to the new standard within the coexistence window.

Swift's Transaction Manager (TM) platform is closely related to ISO 20022. In 2019, Swift revealed plans to develop this platform in a push to move away from traditional sequential messaging to a system that allows every participant in a transaction to have an end-to-end and up-to-date view on the status of the transaction. In addition to operational advantages, the TM platform will play an important role in supporting financial entities that have not completed migration to ISO 20022 by the end of the coexistence period.

By moving from secure message forwarding to end-to-end transaction management, Swift wishes to use richer data and reduce friction (i.e. provide a better customer experience, enhance efficiency and include value-added services such as transaction validation). The underlying communication channel for a transaction is format agnostic and can be FIN MT, ISO 20022 MX, or a combination of channels based on the capabilities of the transaction parties involved (i.e. backward compatibility). The platform ensures full transaction data accessibility to any authorised party in the transaction chain, thereby helping to ensure end-to-end transparency. In the future, Transaction Manager may also help facilitate the use of application programming interfaces (APIs) so that authorised users can retrieve the status of their transaction via an API call over the Swift network.

Swift's Transaction Manager went live in November 2022 and started processing live customer traffic in May 2023. By the end of September 2023, full-service availability had been achieved, with 100 % of ISO 20022-originated payments being processed by Transaction Manager.

4.2.4 Swift's contribution to the G20 roadmap for enhancing cross-border payments

In 2020, the G20 announced the Roadmap for Enhancing Cross-border Payments, which includes several actions to improve the speed, cost, transparency, choice of and access to cross-border payments. From the outset, Swift supported the objectives set out in the roadmap in several ways.

One example is the aforementioned industry-wide migration to ISO 20022, launched in March 2023, which is setting the stage for new levels of operational efficiency and innovation. In fact, Swift's Payments Market Practice Group (PMPG) was directly involved in a workstream focused on improving data quality and straight-through processing by enhancing data and market practices. The adoption of a common message format, such as ISO 20022, should play an important role in ensuring payment system interoperability and, more generally, in addressing data standards and quality and quantity restrictions in cross-border payments.

A joint task force consisting of banks and financial market infrastructures, sponsored by the PMPG, has developed preliminary harmonisation guidelines with the aim of setting minimum requirements for core data components across the cross-border payments chain. These guidelines could serve as best practice requirements for ISO 20022 messaging in cross-border payments after the co-existence phase ends in 2025.

According to analysis of payment exceptions by Swift, formatting issues, account issues and invalid data are major sources of friction in the area of cross-border transactions. Much of this friction could be avoided by checking payments for errors before they are sent. To that end, Swift offers Payment Pre-validation, a service that allows users to check for typos and formatting errors upfront to ensure payments go through the first time. This service continued to gain momentum in 2023, with around 300 financial institutions having signed up.

Launched in 2017, the Swift Global Payments Initiative (GPI) gained traction as the new standard for cross-border large value payments. Swift GPI combines traditional Swift messaging with a new set of rules. Any financial institution adhering to the GPI has to follow these rules, which provide for transparency of fees, end-to-end payment tracking, and confirmation of credit to the recipient's account. Each transaction is assigned a unique end-to-end transaction reference (UETR) which payment providers can use to trace the transfer from start to finish.

The benefits for GPI customers are numerous. Firstly, GPI substantially increases payment speed by eliminating payment friction and reducing the risk of delays through upfront account verification. Another way GPI reduces friction is through automated exception management processes, allowing users to handle queries between banks on the Swift network and resolve instances of incorrect or missing payment information.

Financial crime compliance (FCC) is another important aspect for participants in cross-border transactions. FCC offers a portfolio of financial crime compliance solutions that help member institutions navigate more complex compliance requirements.

As such, GPI fits into Swift's strategy of ensuring fast and frictionless messaging services. As the benefits of GPI are realised leveraging Swift's existing messaging infrastructure, users can expect the same level of security and resilience as when using traditional Swift messaging services.

Whereas Swift GPI facilitates high-value or wholesale cross-border payments, Swift Go aims to ensure fast and frictionless low-value international payments, another key objective of the G20 roadmap. Introduced in July 2021, Swift Go is an interbank service that makes it quicker and cheaper for participating banks to send low-value cross-border payments, with the possibility of instant settlement. It allows sending banks to fully customise their front end to offer customers an easy and intuitive payment experience. As such, Swift wishes to ensure that the traditional banking sector remains competitive in the high-growth market for low-value cross-border payments.

Swift Go builds on the rails of Swift GPI to facilitate speedy cross-border payments. It leverages enhanced service levels between banks, a single payment format and pre-validation services, ultimately removing delays caused by friction in the transaction chain. In addition to faster payments, Swift Go offers more competitive processing fees, enhanced transparency, greater predictability, and payment tracking, combined with the security that users have come to expect from Swift. More than 600 customers had already signed up for Swift Go, with more than 450 banks testing the service or technically live, at the end of 2023.

The services and products outlined above illustrate Swift's eagerness to support the industry's push towards enabling faster, cheaper, more accessible and transparent payments. Swift is continuously examining and developing advanced capabilities for its service offering for both payments and securities, improving end-to-end transaction processing and helping banks and financial institutions deliver the high-quality services their customers expect.

In September 2023, Swift announced that it would introduce Swift Essentials, a portfolio of value-added services, including GPI, Swift Go, Pre-validation, Swift Transaction Screening and Swift Payment Controls. Since 1 January 2024, Swift Essentials has been universally applied to all Swift users in scope, entitling them to take up any components or value-added services in the portfolio, with a single annual invoice issued for all services included in Swift Essentials.

To properly inform its user community, Swift conducted a Swift Essentials awareness campaign throughout 2023, reaching out to the community and specific clients.

4.3 Focal points for Swift oversight in 2024

The annual planning of Swift oversight is guided by a risk-based approach. The oversight risk assessment is intended to help maximise the effectiveness and efficiency of the review. The 2023 assessment was used as a basis for 2024 planning. After each quarter, overseers evaluate the topics analysed and decide which require deeper review or possibly additional information from Swift. This approach gives overseers the flexibility to dedicate more time to particular topics, where appropriate, or to coordinate follow-up discussions at a later stage.

Swift operates in a changing environment characterised by increasing competition and rapidly evolving technologies. This context affects its go-to-market strategy (e.g. new product offerings and a shift towards agile software development) and operations (e.g. the software development lifecycle, incident management and business continuity). Furthermore, an appropriate strategy should be set to tackle a range of emerging challenges, such as geopolitical issues, the global scarcity of skilled resources and the changing cyber-threat landscape. Overseers are aware of the pace of change and will continue to monitor how it affects Swift in terms of technology planning, resilience guarantees, risk assessment, security decisions and design choices, while keeping the global user base properly informed. Overseers seek assurance at all times that the risks identified as arising from new technology choices and major projects are adequately managed and mitigated, to ensure business continuity with comparable or better resilience.

Cybersecurity strategy and risk management remain major topics on the agenda of overseers for 2024. Overseers are analysing which security investments and enhanced capabilities will contribute to protecting Swift against increasingly sophisticated cyberattacks. The cybersecurity review also entails challenging the ISAE 3000 reports by Swift's external security auditor. These reports provide independent assurance on Swift's internal policies, procedures and controls structured around the five sets of HLEs. The ISAE 3000 reports include rich information important to the oversight of Swift and are thoroughly reviewed each year.

The software development lifecycle (SDLC) is intricately connected to both security and operational resilience within an organisation. Throughout the various phases of the SDLC, security measures can be integrated to identify and address vulnerabilities, ensuring that customer-facing product offerings developed by Swift are resilient to potential threats. By incorporating security considerations such as requirements and design as early as possible, organisations can proactively mitigate risks and enhance the overall security posture of their systems.

Change management is another closely related topic. Change management processes are designed to control and manage modifications to the ICT environment, which is essential to maintaining secure and stable infrastructure. Change management relates to the focus on implementing alterations to software after its initial release as changes introduced during the software development process require careful consideration to avoid disruptions, maintain system integrity, and ensure alignment with organisational goals. Proper oversight is crucial to the collective monitoring of these processes as it ensures that changes are systematically evaluated, approved

and integrated into the software, thereby preventing potential issues and guaranteeing stability, security and functionality.

Due to a slight uptick in service availability-related issues in the recent past, overseers will continue to monitor and refine policies and processes related to problem and incident reporting by Swift.

Follow-up of the CSP is also on the oversight agenda for 2024. The Swift user community's level of compliance with CSCF controls, developments concerning customer cases, the results of the new cycle of mandatory independent assessments, and the CSPAC initiative are of particular interest from an oversight perspective. The Bank, in its capacity as lead overseer, will use the in-person Swift Oversight Forum meeting to provide an update on the proposed changes to the CSCF. In doing so, the overseers seek to encourage other national authorities and supervisors to continue to push supervised institutions to improve their endpoint security and to leverage the capabilities of KYS self-assessment data in their oversight toolbox.

Finally, the outcome of the OSR of third-party risk management resulted in a few observations which will require Swift to take appropriate follow-up actions. The TG will monitor the implementation of these actions and mitigating measures in the coming year. Swift has defined new processes to monitor third-party risks based on recently published best practices. The gradual migration of its existing (critical) vendor base to the new approach will be a focus area for TG activities in 2024.

Oversight planning for 2024 is structured around the five HLEs, which serve as the starting point when selecting topics for review. In accordance with the risk-based approach, the previous year's assessment forms the basis for the coming year's review activities. For 2023, this resulted in an extensive list of topics to be analysed by overseers, of which the major ones were:

- HLE 1: Risk Identification and Management
  - Swift's overall risk profile and topic-specific risk assessments
  - Development of an enterprise-wide governance risk & compliance tool
  - Internal and external audit findings and identified mitigating actions

- HLE 2: Information Security
  - Data confidentiality, integrity and availability, including the quantum cryptography roadmap
  - Threat-led penetration test (red-team) outcomes

- HLE 3: Reliability and Resilience
  - Incident management and business continuity
  - Implementation of change management practices

- HLE 4: Technology Planning
  - ICT technology roadmap and investment drivers
  - New product and service offerings and collaboration between Swift and the industry

- HLE 5: Communication with Users
  - Outreach to the global user community
  - Appropriate collaboration with the global user base to increase the resilience of end-users

Themed articles

5. Digital operational resilience

Thomas Plomteux

The European regulation on digital operational resilience for the financial sector (the Digital Operational Resilience Act or DORA) entered into effect on 16 January 2023.[1] The provisions of DORA will apply as of 17 January 2025.

The impetus for this regulation was the industry's ever-increasing dependence on digital assets and processes. As a result, ICT risks pose a growing challenge for the operational resilience, performance and stability of the European financial system. In addition, the European Commission considered that previous legislation did not address this issue in a sufficiently detailed and comprehensive manner, did not provide financial supervisors with the most adequate tools to fulfil their mandate, and left too much room for divergent approaches within the EU single market. The European Supervisory Authorities (ESAs) had also issued joint technical advice calling for a more coherent approach to the management of ICT risks in the financial sector.

DORA is based on five pillars:

- The first pillar consists of key principles and requirements on ICT governance and risk management, inspired by relevant international and sectoral standards, guidelines and recommendations. These requirements concern specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, training and development, and communication) and underline the importance of an adequate policy and organisational framework. This pillar also covers the crucial and active role to be played by the management body in driving forward the ICT risk management framework and assigning clear roles and responsibilities for ICT-related functions.
- The second pillar contains requirements related to the management and classification of ICT-related incidents as well as provisions to harmonise and streamline the reporting of major incidents to the competent authorities. In addition, this pillar addresses the responsibility of competent authorities to provide feedback and guidance to financial entities and to transmit relevant data to other authorities with a legitimate interest. The aim is for financial entities to have to report major incidents to a single competent authority. In this context, the feasibility of an EU hub will also be examined by the ESAs, the ECB and the European Union Agency on Cybersecurity (ENISA). Last but not least, the incident reporting obligations under PSD2 will be fully integrated into this new reporting framework.
- The third pillar concerns the requirements for testing digital operational resilience, i.e. periodically assessing resilience to cyber-attacks and identifying weaknesses, shortcomings, or gaps, as well as the rapid implementation of corrective measures. While all financial entities are required to subject their ICT systems to testing, which can range from scanning for vulnerabilities to analysing software, only those entities identified by competent authorities will be required to perform advanced threat-led penetration testing (TLPT).
- Fourth, the regulation contains provisions to ensure proper management of third-party ICT risks. On the one hand, this objective will be achieved by imposing rules on how financial entities should monitor these risks and by harmonising key elements of the provision of services and the relationship with external ICT service

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

providers. On the other hand, the regulation aims to promote convergence in supervisory approaches to third-party ICT risks in the financial sector by establishing an EU oversight framework for critical third-party ICT service providers.

- The fifth and final pillar aims to increase awareness of ICT risks and related aspects. This pillar focuses on limiting the spread of these risks and supporting defensive capabilities and threat detection techniques, while explicitly allowing financial entities to establish mutual arrangements for information exchange on cyber threats.

With a view to achieving maximum harmonisation in the financial sector, DORA targets a wide range of financial entities, including central securities depositories, credit institutions, insurance and reinsurance companies, stockbroking firms, payment institutions and electronic money institutions.

DORA should be considered a *lex specialis* with regard to the EU directive on measures to ensure a high common level of cybersecurity in the Union (also referred to as the NIS 2 Directive).[1] This means that DORA's requirements, for example regarding ICT security or incident reporting, are at least equivalent to those of the NIS2 Directive and that institutions falling under DORA need only comply with the provisions of this regulation unless – which is not expected – the national legislation transposing the NIS2 Directive explicitly extends the directive's scope or provisions.

Given the strong link between the digital and physical resilience of financial entities, the obligations set out in Chapters III and IV of the Critical Entities Resilience Directive (CER)[2] do not apply to financial institutions covered by DORA either. Here, too, though, the national legislation transposing the CER Directive could expand the scope or provisions of the same.

The Bank is committed to ensuring the successful implementation of DORA:

- On the one hand, the Bank is actively contributing, under the auspices of the ESAs, to the creation of level 2 standards to clarify DORA in many areas. A first set of draft standards covering the ICT risk management framework, the criteria for classifying ICT-related incidents, the policy regarding ICT services offered by third parties that support critical or important business functions, and the templates to be used when reporting ICT third-party dependencies to the competent authorities has already been released. Most of these standards have since been adopted by the European Commission via delegated acts (not yet published in the Official Journal).[3] A second set of draft standards should be finalised by 17 July 2024 and will include provisions related to the reporting of major ICT-related incidents, advanced threat-led penetration testing, subcontracting of ICT services supporting critical or important business functions, and the oversight of critical third parties. The public consultation on this second set of standards ran until 4 March 2024.[4] More information on DORA-related policy mandates and instruments can be found in Box 9.
- On the other hand, the Bank is strongly committed to the successful implementation of DORA through increasing awareness in the sector by means of various seminars, communications and surveys; facilitating the integration of DORA into the Belgian legal order; developing the necessary ICT tools and processes for data collection and dissemination; adapting existing supervisory methodologies; and anticipating, insofar as possible, the impact that the oversight of critical third parties will have on its activities.

1 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

2 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

3 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party.

4 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-launch-joint-consultation-second-batch-policy-mandates.

BOX 9

DORA policy instruments

DORA lays down several mandates for the European Supervisory Authorities (ESAs), in some cases in consultation or in agreement with the European Union Agency on Cybersecurity (ENISA) and/or the European Central Bank (ECB), to give form to the Level 1 text through common draft regulatory or implementing technical standards (RTS or ITS), guidelines and a report. Moreover, the European Commission has called on the ESAs for advice on two Commission delegated acts under DORA. The table below presents an overview of these mandates.

ICT risk management (chapter II)	ICT-related incident management, classification and reporting (chapter III)	Digital operation resilience testing (chapter IV)	Management of ICT third-party risk (chapter V, section 1)
RTS on ICT risk management framework (Art. 15)	RTS on criteria for the classification of ICT-related incidents (Art. 18(3))	RTS to specify threat-led penetration testing (Art. 26(11))	ITS to establish the templated for the register of information (Art. 28(9))
RTS on simplified ICT risk management framework (Art. 16(3))	RTS to specify the reporting of major ICT-related incidents (Art. 20(a))		RTS to specify the policy on ICT services provided by third parties (Art. 28(10))
Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents (Art. 11(11))	ITS to establish the reporting details for major ICT-related incidents (Art. 20(b))		RTS to specify the elements to determine and assess when subcontracting ICT services supporting a critical or important function (Art. 30(5))
	Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21)		
			Managing of ICT third-party risk (chapter V, section 2)
			Call for advice on criticality criteria and oversight fees
			Guidelines on cooperative ESAs-NCA regarding DORA oversight (Art. 32(7))
			RTS on harmonisation of oversight conditions (Art. 41)

Policy mandates with the deadline of 17 January 2024 (first batch)	Policy mandates with the deadline of 17 July 2024 (second batch)

Source: NBB.

The remainder of this box describes these policy mandates and their current status in more detail. This overview is based on the DORA Level 1 text, [1] the draft policy instruments, and information published on the websites of the ESAs [2, 3, 4] and the European Commission. [5]

Call for advice on criticality criteria and fees

In December 2022, the Commission issued a call for advice to the ESAs in relation to two delegated acts under DORA, in order to specify further the criteria to designate critical ICT third-party service providers (subject to the EU oversight mechanism) and to determine the fees levied on such providers and the way in which they are to be paid. The ESAs published their joint response to the Commission on 29 September 2023. [6] In turn, the Commission published draft acts for public consultation (between 16 November and 14 December 2023). [7] The final acts were adopted by the Commission in the first quarter of 2024.

Quantitative and qualitative indicators have also been proposed in relation to criticality criteria, along with the necessary information to build up and interpret such indicators using a two-step approach. Minimum relevance thresholds have been put forward for the quantitative indicators, to be used as starting points in the assessment process to designate critical third-party providers.

In addition, the proposals clarify the types of estimated expenditures to be covered by oversight fees, the information to be used to determine the applicable turnover of CTPPs, the calculation basis and method, and practical issues relating to fee collection. Provision is also made for a financial contribution for voluntary opt-in requests.

First batch of regulatory and implementing technical standards

The technical standards mandated by DORA can be grouped into two batches depending on their deadline for submission to the European Parliament, the Council and the Commission. The first batch of final reports on proposed draft regulatory technical standards and implementing technical standards was published by the ESAs on 17 January 2024 and submitted to the European Commission, which has adopted most of these documents (i.e. the regulatory technical standards) via delegated acts.

The *RTS on ICT risk management framework and on simplified ICT risk management framework* identify further aspects related to ICT risk management with a view to harmonising tools, methods, processes and policies, complementary to those identified in the DORA Level 1 text. They further identify the key elements that financial entities subject to the simplified regime and of lower scale, risk, size and

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

2 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party.

3 See https://www.eba.europa.eu/publications-and-media/press-releases/esas-launch-joint-consultation-second-batch-policy-mandates.

4 See https://www.esma.europa.eu/press-news/esma-news/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party.

5 See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13980-Critical-ICT-third-party-service-providers-criteria-fees_en.

6 See https://www.esma.europa.eu/press-news/esma-news/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party

7 See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13980-Critical-ICT-third-party-service-providers-criteria-fees_en.

complexity will need to have in place and set out a simplified ICT risk management framework. There are a number of changes to the text as compared with the version that underwent public consultation, primarily relating to the introduction of further proportionality and, where possible, a risk-based approach; the removal of an article on governance and information security awareness from the general regime requirements (as a mandate for this was considered not to be included in the DORA Level 1 text); and the clarification of certain provisions, especially those in the articles on network security, encryption, access control and business continuity.

The *RTS to specify the policy on ICT services supporting critical or important functions* specify certain aspects of the governance arrangements, risk management and internal control framework that financial entities should have in place when working with ICT third-party service providers. They aim to ensure that financial entities remain in control of their operational risks, information security and business continuity throughout the lifecycle of contractual arrangements with ICT third-party service providers. The proposal submitted for public consultation was only amended to a limited extent. For example, it was clarified that the policy will apply to subcontractors for ICT services that support critical or important functions or material parts thereof, and financial entities will be given more leeway in updating their contractual arrangements with third-party service providers when review of this policy requires such updates.

The *RTS on classification of major incidents and significant cyber threats* specify the criteria and approach for the classification of major ICT-related incidents, the materiality thresholds of each classification criterion, the criteria and materiality thresholds for determining significant cyber threats, the criteria for competent authorities to assess the relevance of incidents for competent authorities in other Member States, and the details of the incidents to be shared with the latter. Compared with the version that was submitted by the ESAs for public consultation, significant changes have been made to the classification approach, the specification of the classification criteria and their thresholds, and the reporting requirements for recurring incidents, to introduce more proportionality, address issues raised by the financial sector and cover relevant cyber incidents.

The draft ITS on the register of information set out the templates to be maintained and updated by financial entities in relation to their contractual arrangements with ICT third-party service providers. The register of information will play a crucial role in the ICT third-party risk management framework of financial entities and will be used by competent authorities and ESAs in the context of supervising compliance with DORA and to designate critical ICT third-party service providers subject to the DORA oversight regime. Compared with the version that formed the object of public consultation, the information to be registered has been reduced and templates have been streamlined, financial groups will be allowed to use a single register as long as they are capable of fulfilling their reporting requirements to the competent authorities, and it has been clarified that financial entities will be required to document in the register those subcontractors that effectively underpin ICT services supporting critical or important functions or a material portion thereof.

Second batch of regulatory and implementing technical standards

A second batch of technical standards is due to be submitted to the European Parliament, the Council and the Commission by 17 July 2024. Proposals for these policy instruments were subject to public consultation from 8 December 2023 until 4 March 2024. This batch includes the following mandates.

The *draft RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents* cover the content of major incident reports, the time limits for their submission and the content of the notification of significant cyber threats. They also ensure consistency with the incident reporting approach of the NIS2 Directive. With regard to the content of major incident reports, the draft RTS aim to strike an appropriate balance between providing competent authorities with essential information about each incident and not imposing a reporting burden on financial entities. With regard to the notification of significant cyber threats (to be reported on a voluntary basis), the draft RTS provide for short, simple and concise content.

The *draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat* cover aspects related to general reporting requirements and introduce the format and templates for reporting major incidents and significant cyber threats under DORA. With regard to the template, the draft ITS provide for a single template covering the initial notification as well as intermediate and final reports. The draft ITS also provide a data glossary, characteristics of the data fields and instructions on how to populate them.

The *draft Guidelines on aggregated costs and losses from major incidents* specify the estimation of aggregated annual costs and losses caused by major ICT-related incidents. They introduce reporting on gross costs and losses, financial recoveries and the net costs and losses caused by such incidents. The guidelines also propose basing the reference period for aggregation on an accounting year in order to rely on available figures from validated financial statements.

The *draft RTS on threat-led penetration testing (TLPT)* further specify the criteria to be used to identify financial entities required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, the methodology and approach for each testing phase, the results, the closure and remediation stages, and the type of supervisory and other relevant cooperation needed for implementation of TLPT and the facilitation of mutual recognition.

The *draft RTS on subcontracting of critical or important functions* specify the points that need to be determined and assessed when outsourcing ICT services supporting critical or important functions (or material parts thereof). The draft RTS follow the lifecycle of arrangements between financial entities and ICT third-party service providers when subcontracting ICT services supporting critical or important functions and set key requirements for financial entities in this regard, covering the risk assessment before ICT services supporting critical or important functions can be subcontracted, the contractual arrangements, the monitoring of subcontracting arrangements, information on material changes, and exit and termination rights.

The *draft Guidelines on oversight cooperation between ESAs and competent authorities* cover the detailed procedures and conditions for the allocation and execution of oversight tasks between competent authorities and the ESAs and details on the exchange of information (for instance regarding the designation of critical ICT third-party service providers or to ensure the follow-up of recommendations addressed to such providers).

The *draft RTS on oversight harmonisation* specify the information to be provided by ICT third–party service providers when making a voluntary request to be designated as critical; the content, structure and format of the information to be disclosed or reported by ICT third-party service providers; and the

details of the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on the oversight recommendation. The mandate for the joint examination teams will be finalised in accordance with a slightly different timeline.

Feasibility report on an EU hub

Finally, the ESAs are tasked with assessing, in consultation with the ECB and ENISA, the feasibility of and conditions for the potential centralisation of ICT-related incident reporting at EU level. Such centralisation could take the form of a single EU hub for major ICT-related incident reporting, which could either receive relevant reports directly and in turn automatically notify national competent authorities or merely centralise relevant reports forwarded by national competent authorities, thus performing a coordinating role. A report on this topic will be submitted to the European Parliament, the Council and the Commission by 17 January 2025. With that in mind, the proposed EU hub will not, in any case, be operational at the time DORA becomes applicable to financial entities.

6. The impact of interest rate volatility on Euroclear Bank and BNYM SA

Emilie Decembry & Ingmar Vansieleghem

Central banks around the world maintained low, or even negative, interest rates to boost subdued economic growth during and after the pandemic. These low interest rates affected the net interest income of financial institutions, which saw their interest margins collapse. Soaring inflation linked to the war in Ukraine ushered in successive central bank rate hikes, with policy rates being raised by up to 500 basis points between early 2022 and the end of 2023. This allowed financial institutions to restore normal interest margins and stabilise their net interest income. Financial market infrastructures (FMIs) are less reliant on net interest income due to the specific nature of their business model, which is not focused on attracting client deposits. Such deposits can however remain (overnight) on the books of FMIs due to client cash management inefficiencies or pre-financing needs. In the management of an FMI's balance sheet, client deposits are typically reinvested on the interbank market or with central banks. Institutions such as Euroclear Bank and BNYM now receive a positive interest rate on deposits held at central banks, while this rate was previously negative.

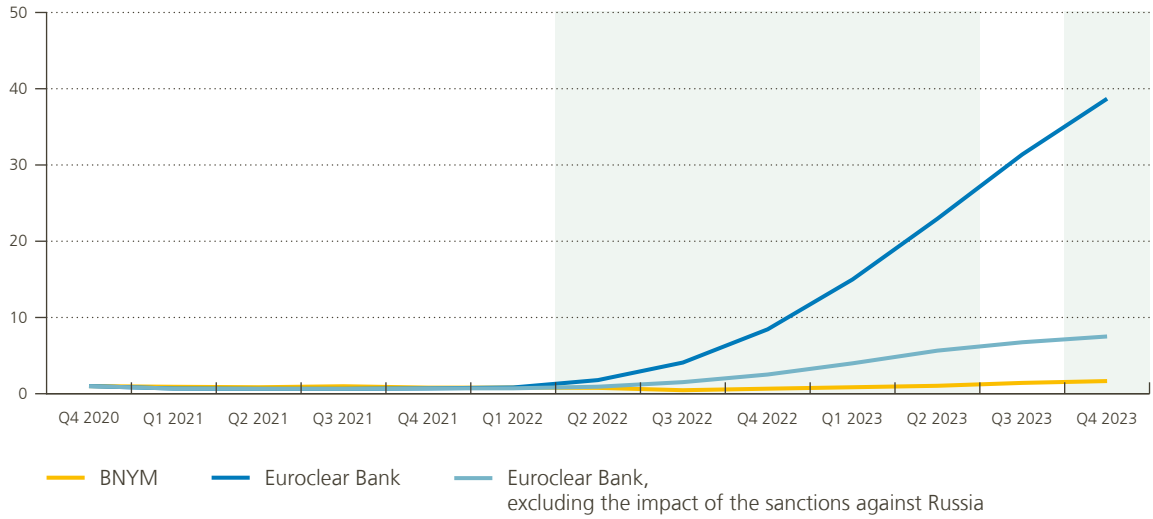
Euroclear Bank, a central securities depository (CSD), has incentives in place for clients not to leave deposits with it (overnight). When central banks applied negative interest rates, the rates Euroclear Bank charged its clients were below those of central banks. After the interest rates hikes, Euroclear Bank is once again applying a zero interest rate. BNYM SA now applies a positive interest rate.

The figures below show the (indexed average) change in the quarterly net interest income of Euroclear Bank and BNYM. For Euroclear Bank, a distinction is made between business-as-usual net interest income, on the one hand, and net interest income including the impact of the sanctions against Russia, on the other hand. Compared with 2020, net interest income increased slightly for BNYM but far more significantly for Euroclear Bank (Figure 8). At BNYM, net interest income accounted for 25 % of operating income on average by the end of 2023 – compared with 10 % to 15 % in 2022 (Figure 9). Euroclear Bank reported a higher ratio of net interest income to net operating income. This was mainly due to reinvestment of the proceeds from frozen Russian assets.

Figure 8

Average quarterly net interest income

(indices, December 2020 = 1, ECB rate hike periods are shaded)

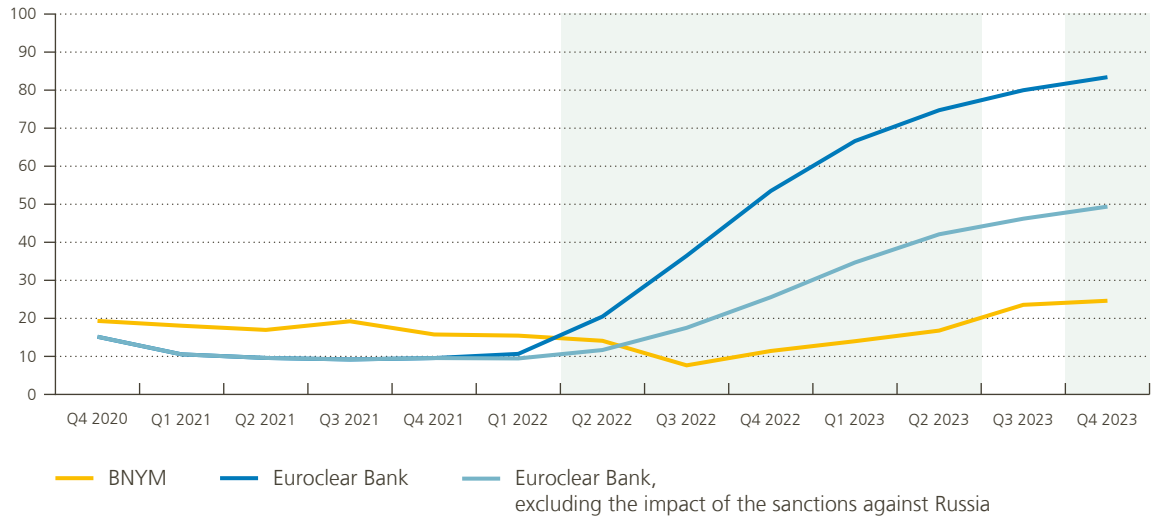


Source: NBB.

Figure 9

Ratio of average quarterly net interest income to average quarterly operating income

(in %, ECB rate hike periods are shaded)



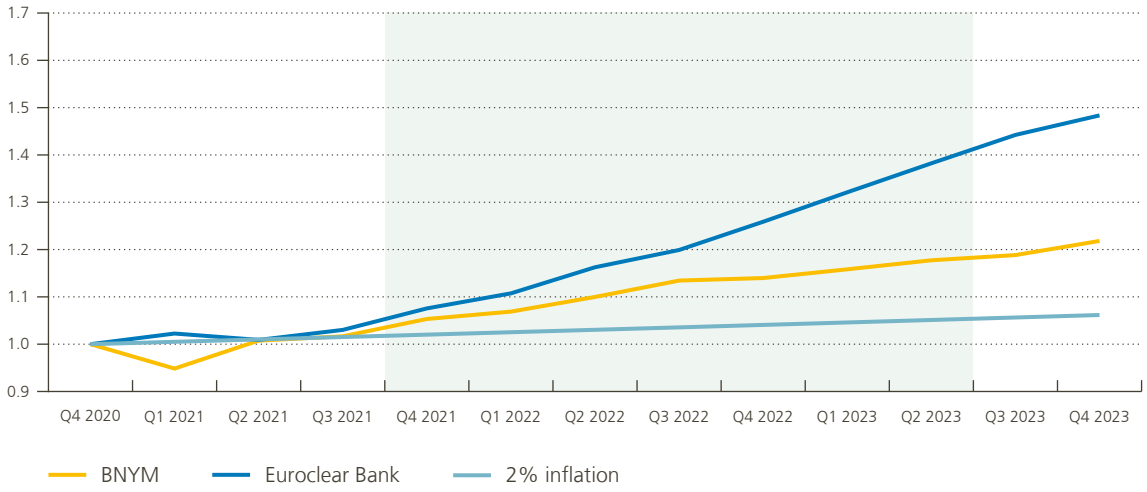
Source: NBB.

Inflation caused interest rates to rise, with both interest margins and net interest income increasing, and also caused expenses to spiral upwards, due to rising prices and wages. The increase in net interest income helped to cover higher administrative costs. As shown in Figure 10 below, such costs rose at a faster pace for Euroclear Bank than for BNYM – 50 % for Euroclear over three years compared with 22 % for BNYM – due, among other factors, to costs related to the management of frozen Russian assets.

Figure 10

Average quarterly administrative expenses

(indices, December 2020 = 1, periods of high inflation, i.e. above 5%, are shaded)



Source: NBB.

By the end of June 2023, inflation had returned to lower levels and rate hikes were taken off the agenda of central bank monetary policy meetings. The ECB hinted at rate cuts. Indeed, while lower inflation helps stabilise costs, lower interest rates squeeze interest margins on reinvestments and central bank deposits.

7. Environmental and climate-related risks within the FMI landscape

Dorien De Beuckeleer

The Bank continues to monitor climate-related and environmental risks not only for banks and insurance companies[1] but also for financial market infrastructures (FMI), custodians, payment transaction processors and providers of financial messaging services. After a first stocktake in late 2021/early 2022 when a sample of Belgian institutions active in these fields was requested to complete a questionnaire,[2] the Bank decided to continue interaction with these institutions and to analyse climate-related and environmental risks in a structural manner. This structural follow-up includes both firm-specific and horizontal analyses, as well as a combination of global reviews and in-depth analyses of selected areas impacted by climate-related and environmental risks (see the 2023 FMI Report[3] for more information on the areas in which the Bank is focusing its climate-related reviews).

During the first stage of this structural follow-up, the Bank sent a questionnaire to a sample of FMIs, custodians, payment transaction processors and providers of financial messaging services. Based on the answers received, the Bank performed a global review of the maturity of these institutions in the areas referred to above (e.g. assessment of the materiality of various climate-related risks, the impact of climate-related risks on the business model, etc.). This assessment consisted of two parts, the first of which entailed a firm-specific analysis of maturity in each area. When performing this maturity assessment, the Bank took into account the expectations set out in the 2023 FMI Report.[4] Next, a comparison of the institutions and an analysis of the horizontal trends, similarities and differences observed was performed. This article presents the results of the maturity assessment as well as general trends and sector-wide observations for each aspect. It should be noted that the assessment and sector-wide observations are based on the answers provided by institutions to the questionnaire. The underlying documentation and other forms of evidence complementing the self-assessment will be analysed in the context of in-depth, topic-specific reviews, to be carried out in the coming years.

The assessment found that climate-related risks are adequately embedded in the governance framework of the institutions surveyed, thereby demonstrating their awareness of climate-related risks, but that the appropriate integration of such risks in the risk management framework and business strategy remains an area for improvement. Most institutions have an adequate to strong level of understanding of the materiality of climate-related risks and make public disclosures on such risks. They have processes in place to capture climate-related risks in their materiality assessments, but there are substantial differences in terms of the extent to which these risks are embedded in the enterprise risk framework. Climate-related risks are embedded in a high-level or *ad hoc* fashion in the business strategy and risk management of all institutions concerned, and improvements are

1 See the "Prudential regulation and supervision" section of the Bank's Annual Report 2023, available at https://www.nbb.be/doc/ts/publications/nbbreport/2023/en/t1/report_2023_t1_complet.pdf.
2 See https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2022/fmi-2022_climate.pdf.
3 See https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2023/fmi-2023_brexit.pdf.
4 See https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2023/fmi-2023_brexit.pdf.

generally needed in order to achieve full, structural integration. Several institutions are currently implementing or have plans to implement actions to enhance the integration of climate-related risks in various aspects of their internal organisation.

The institutions surveyed did not identify potential risks in the short term, but rather listed potential impacts in the medium to long term, mainly related to operational, business and reputational risks. From a governance perspective, climate-related risks have been embedded at different levels of each organisation, from the operational level to the board level.

In terms of potential business-specific effects, institutions identified many different possible impacts, ranging from higher costs and changes at the product level to business disruption and consequences for employee availability and reputation. Mitigating actions are mainly being carried out in the areas of measuring and monitoring and energy (cost) savings, as well as through third party-related initiatives (e.g. factoring ESG aspects into the assessment of new suppliers and clients, collaboration with suppliers to reduce the impact of greenhouse gas emissions throughout the value chain, etc.). The direct impact of FMIs' own activities on climate change is typically less significant than in other sectors. Nonetheless, the institutions surveyed distinguished three different ways in which they could tackle climate-related risks: (1) taking actions to reduce their own emissions, (2) encouraging stakeholders to reduce their impacts and (3) developing and adjusting products and services to help customers meet their climate-related goals. Certain institutions have already developed key performance indicators (KPIs) and key risk indicators (KRIs) to monitor the impact of climate-related risks on their business while others are in the process of doing so. Existing KPIs and KRIs mainly relate to carbon footprint measurement.

In general, however, climate-related risks are already adequately integrated into business continuity management.

Most institutions publish sustainability-related information on a regular basis, but this information is either quite high level or at an early stage of development for at least some institutions. Institutions have also obtained and published (or plan to publish in the future) one or more external ratings relating to their climate responsibilities.

More information on the analysis is set out below.

Materiality assessment

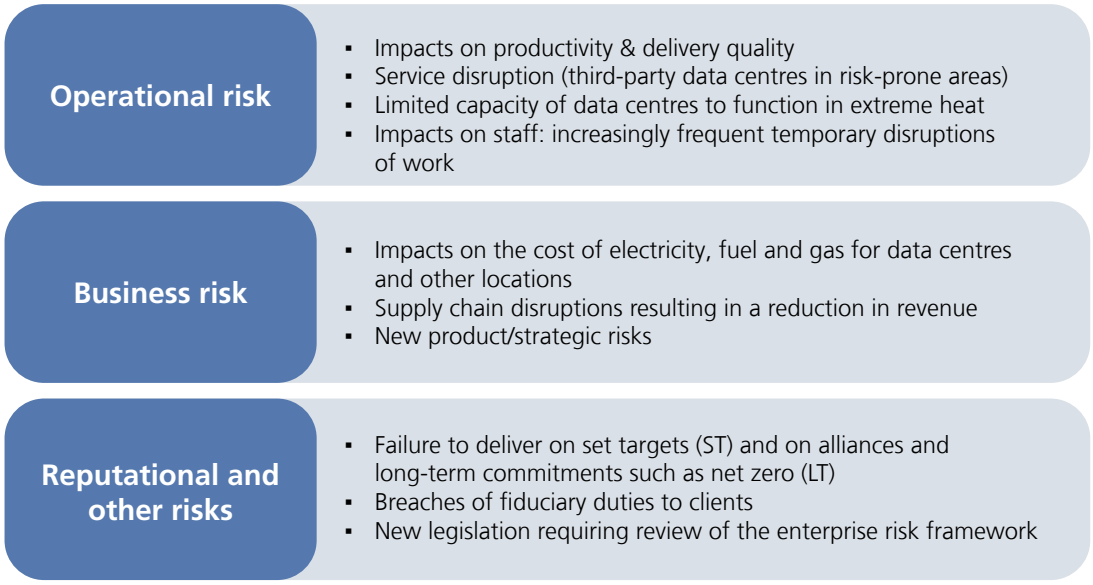
Most of the institutions included in the assessment have an adequate to strong level of understanding of the materiality of climate-related risks and processes in place to identify relevant climate-related risk drivers. They perform regular assessments to identify and assess the materiality of these drivers. These assessments meet a wide range of criteria, such as the tailoring of analyses to the business model and environment, the consideration of different time ranges, etc. Notwithstanding regular materiality assessments, however, the degree to which such risks are embedded in the enterprise risk framework as well as the completeness of these reviews remains an area in which further improvement could be made by some institutions, although institutions mentioned several remediation actions that are currently in progress. Examples of possible enhancements are the inclusion of climate-related risks in the risk library to ensure that the drivers of these risks are considered in annual risk identification and assessment processes, rather than assessing the materiality of climate-related risks solely via *ad hoc* analyses, and the performance of a double materiality assessment[1] on a regular basis. The materiality assessments range from integrating climate-related risks into and aligning them with the risk frameworks and processes that already exist for other types of risks to the introduction of regular, dedicated assessments. The assessments are mostly performed on a yearly basis. Institutions identify few short-term risks, but do list potential material impacts in the medium to long term, which are largely concentrated in three areas: operational risk, business risk (at the level of product development as well as on the cost/revenue side) and reputational/legal/fiduciary risks.

1 A double materiality assessment entails considering both the impact an organisation has on climate and the environment and the impact of climate-related and environmental risks on the organisation.

The diagram below provides some examples of potential risks identified by institutions in their materiality assessments.

Figure 11

Potential risks identified by institutions in their materiality assessments



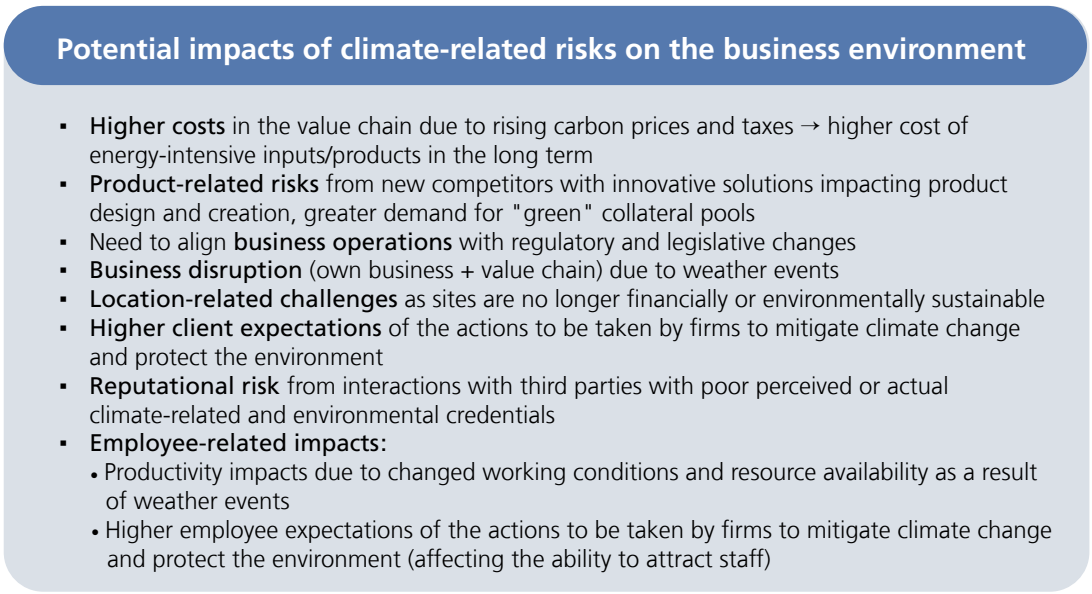
Business environment, business model and strategy

The inclusion of climate-related risks in the business environment, business model and strategy is an area that requires further action. For the most part, climate-related risks are integrated into business management in a high-level manner. In general, the institutions surveyed perform an adequate assessment of the impact of climate-related risks on the business environment in which they operate. Nonetheless, at several institutions, monitoring of the impact of such risks on the business, via key performance indicators (KPI) and key risk indicators (KRI), requires further attention. Progress is expected in this area based on the answers provided to the questionnaire, as the institutions that are the least advanced in this area stated that they are in the process of developing and/or implementing KPIs/KRIs. Current KPIs and KRIs mainly concern carbon footprint measurement and related science-based targets. Some institutions are going a step further and have created a climate-risk dashboard containing a series of reporting metrics covering financial and non-financial risks and impacts. The monitoring of KPIs and KRIs can be complemented by regular point-in-time and forward-looking business model risk assessments which consider the longer-term strategic implications of climate change. The KPIs/KRIs and these strategic assessments are reported to management which incorporate them into strategy-setting processes.

The answers to the questionnaire revealed various potential impacts that climate-related risks could have on the business environment, ranging from higher costs and the need to align business operations to legislative changes, to business disruption and reputational risks. The figure below provides an overview of the potential impacts identified by respondents.

Figure 12

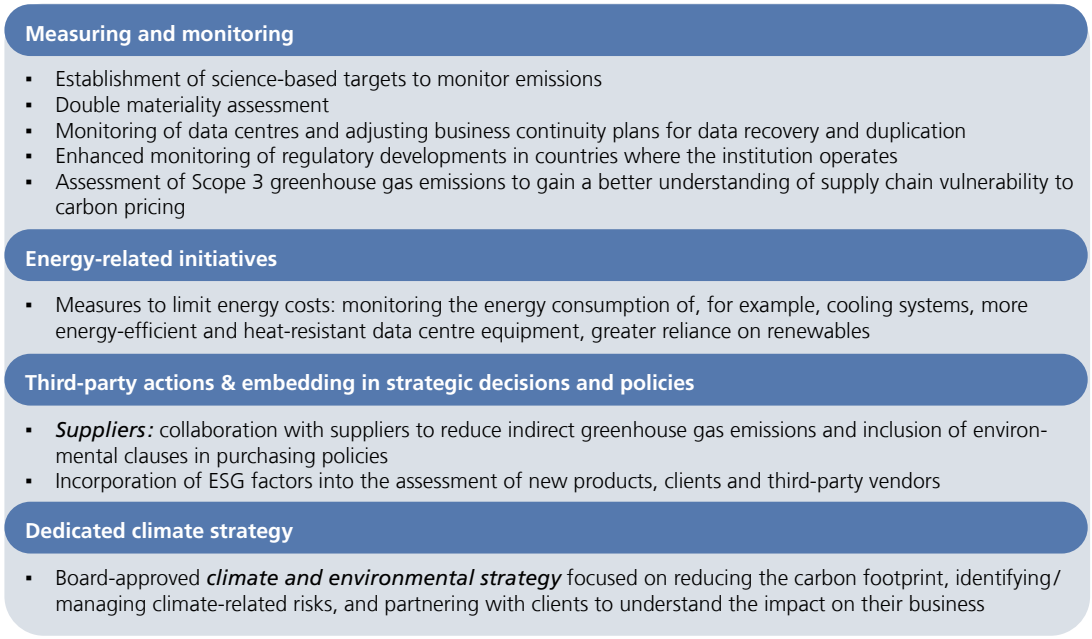
Potential impacts of climate-related risks on the business environment



Institutions have taken actions to mitigate these potential impacts. These actions include measuring and monitoring activities, energy-related initiatives and third party-related actions, the embedding of climate-related aspects in strategic decisions and policies, and the determination and implementation of a dedicated climate strategy. Some examples of the actions taken in these areas are set out below.

Figure 13

Actions taken to mitigate potential impacts on the business environment



1 Scope 3, also called value chain emissions, covers all other indirect emissions which are the result of activities from assets not owned or controlled by the reporting organisation, but that the organisation indirectly impacts in its value chain. Sources include purchased goods and services, transportation, business travel, and employee commuting.

In general, institutions estimate the impact of climate-related risks on their business to be rather limited compared with other sectors. However, they identified three types of actions they can take within the financial sector with regard to climate-related and environmental concerns.

Firstly, they mentioned that they can take actions to reduce their own impacts. In general, institutions intend to take initiatives to optimise the energy efficiency of their operations and to embed ESG in all aspects of their organisation. Examples include setting science-based targets, investing in carbon removal technologies, improving the energy efficiency of buildings, changing travel policies, encouraging employee involvement through the development of dashboards that provide employees with information on certain scope 1[1] and scope 2[2] emissions, adjusting (individual and corporate) printing practices, and taking into account supplier and vendor commitments (to science-based targets) when selecting new commercial counterparties.

Secondly, they believe they can inspire and encourage stakeholders within and beyond the financial community to mitigate climate change. Institutions can communicate on their ambitions to achieve Paris-aligned carbon reduction targets and encourage suppliers to do the same. Due to their central role in the financial sector, they can also put this topic on the agenda of events and conferences they organise. They perform lifecycle assessments to determine which parts of the lifecycle of a product or service have the most impact on climate and the environment and can work to convince other actors in the ecosystem to collaborate, based on the results of these assessments.

Thirdly, institutions can support their customers by offering solutions to help their participants tackle climate-related and environmental risks and achieve sustainability-related targets. For example, CSDs and custodians can support their clients in the issuance, safekeeping and administration of green bonds. Moreover, CSDs and custodians can offer collateral management services to clients in which they can integrate the possibility of adding ESG factors to the collateral eligibility scheme negotiated between the collateral giver and taker. One institution surveyed has integrated ESG elements into the platform where clients register their KYC data and can access their counterparties' KYC data.

Governance

On average, the inclusion of climate-related risks in the governance framework is the area in which institutions have made the most progress. All institutions that completed the questionnaire received an adequate or even strong score in this area. Climate-related risks are integrated at different levels of the organisation, ranging from operational to board level. They are often integrated into the existing organisational structure, such as within certain committees, with committee mandates having been adapted to include climate-related risks (e.g. the designation of a committee member responsible for climate-related risks, changing the nomination committee to the nomination and ESG committee, establishing a social and environmental responsibility committee at board level). These measures are often complemented by additional initiatives, such as the establishment of a multidisciplinary ESG steering committee or the creation of ESG roles to lead and coordinate the implementation of ESG activities across the institution in a consistent manner.

Risk appetite and risk management

Risk appetite and risk management remain areas for improvement when it comes to tackling climate-related risks. Such risks are generally included or considered at a high level or on an *ad hoc* basis in the risk management framework. Most institutions surveyed do not consider climate-related risks to be a separate risk category but rather a driver of other types of risks. Actions are expected, in particular, in the areas of regular measurement and the determination of risk appetite, as the latter exercise is a core part of good risk management. Some institutions

1 Scope 1: all direct CO_2 emissions from the activities of the institution, including on-site fuel combustion.
2 Scope 2: indirect emissions from the generation of purchased electricity, steam, heating and cooling consumed by the institution. These emissions are created during the production of energy.

have already made progress in this area, although points for attention remain such as data challenges (resulting from differences in the methodologies used for data sources), while plans are underway at other institutions to include climate-related risks in their risk appetite. The inclusion of climate-related risks in stress and/or sensitivity testing can also be improved at certain institutions. Climate-related aspects are already considered when performing such activities to confirm the materiality of climate-related risks for business continuity planning and assessment purposes. Such risks are taken into account, for instance, in location management for business continuity purposes.

Institutions also state that they are performing or starting to perform (different types of) assessments along their value chains. For example, ESG factors are included in assessments of new clients, products, processes, third parties and vendors. ESG data obtained from external suppliers (such as Ecovadis)[1] are often used in these assessments. Another example is the establishment of a requirement that suppliers agree, during the onboarding process, to adhere to minimum climate-related and environmental standards.

Disclosures

Most of the institutions surveyed publish sustainability-related information on a regular basis. This information may relate to financial impacts, risks, opportunities, materiality assessments, risk management and key metrics or the role the institution wishes to play. However, the information released tends to be quite high level. Moreover, the institutions surveyed have obtained and/or published one or more external ratings from CDP[2] and EcoVadis or plan to do so in the future.

1 Ecovadis is a provider of business sustainability ratings (www.ecovadis.com).

2 CDP, a non-profit charity, runs a global disclosure system for investors, companies, cities, states and regions to manage their environmental impacts (www.cdp.net).

8. Three typical cyber-attacks: how TIBER-BE approaches threat-led red teaming scenarios

Jean-Louis Buchholz and Samuel Goret

Given the constantly evolving nature of cyber threats, the financial sector faces unprecedented challenges which require innovative testing methodologies. TIBER-EU (Threat Intelligence-Based Ethical Red Teaming for financial institutions in Europe) stands at the forefront, offering a proactive approach to cybersecurity testing. As cyber threats become increasingly sophisticated, financial institutions must prioritise their defence strategies. This article delves into the relevance of TIBER-EU, its focus on critical threats and representative three-scenario approach designed to strengthen the capabilities of institutions to potential cyber adversaries. TIBER-BE, the Belgian implementation of the framework endorsed by the European Central Bank, leverages ethical red teaming to execute realistic cyber threats on live production systems, within legal and ethical boundaries as well as budget and time constraints. Faced with an intricate landscape of threats, TIBER-BE helps institutions pre-emptively address vulnerabilities by employing a customised threat assessment and targeted testing methodology.

Before turning to the three scenarios, it is important to acknowledge the prevailing threats in the financial sector. Advanced persistent threats (APTs) and phishing campaigns are omnipresent. TIBER-BE recognises the need to simulate these threats comprehensively, ensuring financial institutions are prepared to deal with complex modern cyber risks. Insider threat scenarios, although less likely, provide a perfect middle ground to cover tactics and techniques used by a wider variety of malicious actors, without the risk of the test being detected in the early stages of the attack.

The three-scenario approach

TIBER-BE's three-scenario approach orchestrates a strategic progression, starting from sophisticated internal threats and ending with external phishing attacks, an initial access tactic more likely to trigger detection. This reverse order aims to maximise learning by prioritising responses to subtler threats. It should be noted that this approach is customised to the targeted threat intelligence level and specificities of the institution being tested.

Scenario 1: an advanced persistent threat in the form of a "living off the land" attack

Objective: Detect and respond to an advanced persistent threat (APT) deeply embedded in the network. The purpose of the attack could be pre-positioning for espionage, disruption or further compromise of the supply chain.

1. Initial access: simulate a sophisticated attack with unauthorised access to specific infrastructure.
2. Persistence and evasion: establish persistence mechanisms to maintain long-term access and employ techniques such as fileless malware and anti-forensic measures to evade detection.

3. Lateral movement: mimic lateral movement within the network, leveraging legitimate tools to avoid suspicion and opting for "living off the land" tactics and misconfigurations for malicious activities.
4. Data exfiltration: simulate the extraction of sensitive information without triggering alarms and evaluate the institution's ability to detect and respond to data exfiltration attempts.
5. Data/system wipe: introduce or emulate a (controlled) ransomware or data wiping to assess the institution's preparedness and response capabilities to a critical incident.
6. Supply chain intrusion and third-party dependency: simulate the infiltration of the financial institution's supply chain to assess vulnerabilities in external connections and evaluate the impact of an assumed breach on interconnected third-party systems within the supply chain of the financial sector.
7. Response evaluation: assess the speed and effectiveness of the financial institution's response to the breach scenario with a focus on minimising the dwell time of the attacker within the network.

Scenario 2: insider threat

Objective: Identify and mitigate the risks associated with an insider threat with limited hacking capability but legitimate access and insider business or ICT knowledge.

1. Simulated insider access: emulate an insider with restricted access attempting unauthorised actions within the system.
2. Persistence and defence evasion: perform subtle data manipulations to test the institution's ability to detect unauthorised changes and evaluate the effectiveness of the anomaly detection mechanisms. Persistence is trivial given that the threat is an employee or a contractor with legitimate access to the systems.
3. Lateral movement: navigate applications and file sharing to look for misconfigured authorisations, unprotected sensitive data or applications that can benefit from an insider perspective.
4. Covert communication: mimic discreet communication channels to avoid detection and assess the institution's capabilities to detect unusual communication patterns.
5. Incident response: gauge the institution's incident response readiness and evaluate communication and collaboration among response teams.

Scenario 3: phishing and external perimeter attack

Objective: Assess the institution's resilience to a typical external attack, focusing specifically on phishing and attacks targeted at externally exposed assets.

1. Phishing simulation: launch (spear-)phishing campaigns against carefully selected employees to evaluate susceptibility and measure the effectiveness of email filtering and employee awareness training.
2. Malware deployment: simulate malware delivery through phishing vectors and evaluate the institution's static and behavioural endpoint protection and malware detection capabilities.
3. Credential harvesting: emulate credential harvesting techniques to assess the institution's defences against unauthorised access and test the effectiveness of multi-factor authentication.
4. Post-phishing activities: assess the institution's ability to detect and respond to activities following successful phishing attacks and evaluate the speed of isolating compromised accounts and systems.

Conclusion

TIBER-BE's evolving three-scenario approach, enhanced by considerations related to supply chains, enables financial institutions to assess their capabilities in the current cyber threat landscape. By synthesising realistic threat simulations, institutions can develop an effective remediation plan to proactively enhance their cybersecurity resilience and fortify their defences against the emerging challenges of the digital era.

9. Shortening the settlement cycle in European securities markets

Steven Van Cauwenberge

To reduce unnecessary risks and improve efficiency in capital markets, regulators are increasingly focusing on shortening the settlement cycle for securities trades.

With the adoption of the CSD Regulation in 2014, the EU moved from standard settlement of securities trades within three business days from the trade date (T+3) to two business days (T+2), with the US following suit in 2017. The US has now shortened its settlement cycle further and, since the end of May 2024, ensures settlement by the next business day (T+1). The EU is considering doing likewise.

US move to T+1 settlement at the end of May 2024

In February 2023, the US securities regulator (the Securities and Exchange Commission or SEC) introduced rules[1] to move from securities settlement for most broker-dealer trades from T+2 to T+1 by 28 May 2024. The SEC rules apply unless participants expressly agree otherwise. They cover all securities trades with a limited number of exceptions including, for example, municipal and government securities (albeit formally, as US Treasuries are already settled on a T+1-basis), commercial paper and security-based swaps. Derivatives trades are also out of scope, including when linked to money market trades for hedging purposes.

The final stage of a trade conducted on a stock exchange or between counterparties (over-the-counter)[2] is settlement, a process by which securities are exchanged for cash. To allow T+1 settlement, changes are required at both the trade and settlement stages.

Broker-dealers will need to implement policies or enter into written agreements to ensure that trade allocations, confirmations and affirmations with their institutional customers are completed as soon as technologically practicable and in any case no later than the end of the trade day ("same-day affirmation").[3]

After trading, buy and sell instructions must be matched to capture the trade before settlement. Central matching services providers[4] – such as the CSD DTCC in the US and both EU international CSDs – will have to report to the US supervisor on their straight-through processing, so as to allow the timely processing of trades.

1 Available at https://www.sec.gov/files/rules/final/2023/34-96930.pdf.

2 The post-trade settlement process could also include a clearing stage whereby a central counterparty interposes itself between the buyer and the seller.

3 Allocation is the process of assigning executed trades to different accounts or portfolios, ensuring that each account receives the appropriate number of securities. Confirmation is the process whereby the terms of a trade are verified – and confirmed – between the market participants directly involved. Affirmation refers to the same process but between a market participant (e.g. a broker) and their professional customer (e.g. an institutional investor).

4 Central matching service providers help facilitate the processing of institutional trades between broker-dealers and their institutional customers.

Generally speaking, T+1 settlement will not substantially impact settlement by CSDs, given that they already can and do settle the next day (T+1) or even intraday (T+0) in most cases. However, it will clearly impact the operations of market participants (i.e. at settlement level), of CSD participants and of their underlying clients.

For dual listings, trading venues in the EU can continue to use a T+2 settlement cycle for EU trading venues, in line with the CSD Regulation. Nonetheless, dual listing will lead to demands to coordinate corporate events, as their occurrence depends on the settlement period used.

Benefits of moving to a shorter settlement cycle

A shortening of the settlement cycle implies a reduction in counterparty credit risk and related capital costs over the settlement period. When conducting a trade, the buyer has a position in the purchased security from the time the trade is concluded (at day T) notwithstanding later delivery of the security at settlement. Upon delivery, the market price of the security may be higher, and the buyer thus bears, over the settlement cycle, counterparty risk for the cost of the security. All things being equal, the market price of a security will be less volatile over a period of one day than two. To cover this risk, the buyer will need – based on standard distribution assumptions – around 30 %[1] less capital or margin in a T+1 scenario compared with a T+2 scenario.

Market makers need to have cash and securities on hand in order to provide their services. When they do not carry the positions as inventory, they can borrow the securities or cash needed using securities as collateral, although this also requires capital or a margin. The funding possibilities and conditions of the market maker will therefore impact the market liquidity of the securities.

The (costs of the) counterparty and liquidity risks of the market maker will be reflected in the bid-ask spreads they offer. A shorter settlement cycle can be expected to reduce the capital or margin needs for intermediaries and thus diminish bid-ask spreads. Furthermore, a shorter cycle generally reduces the market value of the outstanding transactions trapped and awaiting settlement at any time.

Assuming timely settlement, T+1 settlement will allow the holders of securities to realise cash in a shorter timeframe. This can be especially advantageous in a stressed market in which participants are seeking cash.

From an operational point of view, T+1 settlement will require the industry to use straight-through processing and thus lower operational risk as manual procedures are replaced.

These advantages should be considered against the possible drawbacks and costs.

Costs of moving to a shorter settlement cycle

While it is argued above that a shorter settlement cycle will increase liquidity, the opposite view can be held. A shorter cycle limits the time market makers have to find counterparties. Market makers may incur additional costs to borrow securities or cash which could lead to reduced market liquidity. Also, a broker or CCP may not (fully) reduce the collateral requirement for its counterparties, as it may deem that the period needed to replace a failed trade could take longer than one day.

Also, from an operational point of view, there will be less time to settle trades under a T+1 regime. The industry has indicated that – given customary working hours – the effective window to process a trade after its conclusion

1 This is assuming price changes in the market are normally distributed. Under this statistical assumption, price movements correlate with the length of the settlement period on a "square root" basis, meaning, all other things being equal, reducing the settlement period from two days to one will not halve volatility but reduce it by 30 % (roughly the ratio of the square roots of 1 and 2). This rule of thumb is referred to, for example, in a January 2024 speech on T+1 settlement given by the SEC chair before the EU Commission, available at https://www.sec.gov/news/speech/gensler-speech-prepared-remarks-european-commission-012524.

would diminish by 80 %.[1] To settle on day T+1 requires same-day trade allocation and confirmation, which is challenging for market participants. Operating in a different time zone exacerbates these requirements. Further automation efforts will be needed. Investing in straight-through processing, across a broad range of functions, implies costs. CSDs could be asked to extend their opening hours to allow later cut-off times to accept settlement instructions. Market participants may even consider changing the location of their staff or, alternatively, "operational" outsourcing to local custodians that offer broader services.

A shorter settlement cycle increases the risk of settlement failure. Heightened fail rates – for example, an estimated 15 %-35 % increase in the current fail rates for the US market[2] – are expected to be seen at least temporarily after the transition to a shorter cycle.

Moreover, alignment issues will arise where settlement cycles diverge. The liquidity implications of these may depend on the instrument. For funds, for example, the underlying securities may trade with a diverging settlement cycle, leading to the need for improved cash liquidity and/or securities inventory management.

In addition, a given security could settle on either day T+1 or day T+2 depending on where it trades. This is the case for Euromarket securities listed on both a UK and an EU market. Dealers may reflect their funding costs in their trading prices, resulting in possible differences in bid-ask spreads across trading venues[3].

Finally, when the need arises to source foreign currency liquidity in FX markets that continue to operate on day T+2, risks and costs may increase. There is no corresponding initiative for the FX spot market to shift to T+1,[4] which implies obstacles for investors funding security transactions in a non-domestic currency. In addition, CLS deadlines could be missed, potentially leading to the increased use of bilateral FX settlement.[5]

EU initiatives regarding a move to T+1 settlement

In general, the settlement cycle is determined by the location of the trading venue, not the place of settlement. The securities falling within the scope of an eventual EU decision to move to T+1 settlement are expected to be determined by the scope of the current T+2 requirement. Today, Article 5(2) CSDR sets T+2 as a maximum settlement cycle for securities trades executed on an EU trading venue. Trading parties can – at least in principle – voluntarily agree to a shorter period. Also, counterparties that trade bilaterally can in theory agree on any settlement cycle they wish, including a longer one. The assumption is however that market participants will usually follow the standard set for transactions in the trading venue.

Under the coordination of the Association for Financial Markets in Europe (AFME), a cross-industry working group has been established to study both the impact on EU markets of the US's move to T+1 settlement and the potential migration to T+1 in the EU. The group represents 15 associations of investment managers, trading venues, CCPs, CSDs, broker-dealers, custodians and product-specific experts.

Markets are not expected to move to T+1 settlement on a voluntary basis. Regulatory intervention will thus be required. The CSD Refit Regulation mandated ESMA to produce a report on the costs and benefits of a shortened settlement cycle in the EU. As a first step in this process, ESMA launched a market consultation ("call

1 See the report of the Association for Financial Markets in Europe (AFME) published in September 2022, available at https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_Tplus1Settlement_2022_04.pdf.

2 As referred to in the ESMA feedback statement on its "Call for evidence on shortening the settlement cycle". Fail estimates are discussed on page 27, nos. 99-105.

3 This point is discussed in the report of the UK's Accelerated Settlement Taskforce.

4 Although, notably, the SEC chairman called for considering this in the abovementioned speech.

5 Continuous Linked Settlement (CLS) is a US-based international payment system which was launched in September 2002 for the settlement of foreign currency exchange. Settlements in CLS occur payment-versus-payment and thus avoid principal risk in the event of counterparty default. A CLS press release from early April 2024 deemed the problem to be minimal and in need of further assessment after the US transition to T+1 securities settlement, prior to a decision being taken on possible changes to CLS settlement timelines. See https://www.cls-group.com/news/update-on-the-potential-change-to-clssettlement-timelines-following-the-move-to-tplus1-securities-settlement/.

for evidence") on 5 October 2023. ESMA plans to publish its final report to the Commission at the end of 2024. Quantifying the costs and benefits of a shorter settlement cycle appears challenging.

An EU move to a shorter settlement cycle must be judged on its own merits. The EU market is different than the US or other markets due to a far more fragmented infrastructure, making cross-border settlement, in particular, more complex.

To the extent banks operate globally and markets are interconnected, a worldwide harmonisation of settlement periods could be pertinent. However, the EU does not necessarily need to move at the same time as other jurisdictions. Canada and Mexico will move to T+1 settlement in lockstep with the US, as their markets are clearly interconnected. As the proportion of dual US-EU listings or of EU trades in the US market seems relatively modest, it does not appear absolutely necessary for the EU to move to T+1 settlement at the same time. EU market participants indicate that the UK market's potential move to T+1 settlement would be more relevant to them, as the EU and UK markets are more closely intertwined.

The UK established an Accelerated Settlement Taskforce to analyse this issue, which published a report at the end of March 2024.[1] The report noted a broad consensus to move. It elaborates on the hurdles and requests the establishment of a technical group to further consider the specific details of a move. It envisages a two-step approach for the transition. The move to T+1 settlement, which is planned to take place before the end of 2027, would be preceded by the introduction of a requirement, in mid-2025, for operational processes as well as allocations, confirmations and trade level matching, to take place on the trade date. Finally, the report indicates that while a move to T+0 is not appropriate at this stage, T+1 investments should already bear in mind such an evolution.

Further, the CSD Regulation imposes cash penalties for late settlement on a per transfer basis; this rule was not taken over by the UK when it formally adopted EU legislation at the national level after Brexit. A requirement to settle on day T+1 may increase settlement fails and the ensuing penalties and add to the cost of settlement in the EU.

An EU move will most likely not occur in the next few years as the industry has indicated that it needs at least two years to plan and implement such a decision. Lessons can be learned from other markets moving to T+1 settlement, such as the US. Preparing the transition and industry-wide testing of processing in T+1-mode will be key for market participants. CSDs and the T2S platform may play a role here. Supervisors of CSDs and market participants will be expected to monitor the situation.

Conclusion

Following the move by the US to T+1 settlement, the EU will have to decide whether to move to a shorter settlement cycle. In January 2024, the EU commissioner responsible for financial services, financial stability and capital markets union stated that the question is not if the EU will transition to T+1 but how and when.[2] Back in 1989, the Group of Thirty – a body comprised of industry representatives and central bankers, which recommended T+3 settlement at the time – recognised that "to minimise counterparty risk and market exposure associated with securities transactions, same day settlement is the final goal".[3] Shortening the settlement cycle can bring clear benefits, improve overall efficiency, mitigate credit and liquidity risk and enhance the use of capital. But it is not without costs – at least in the short term – or certain risks that will need to be managed. In 2024, the adoption of (end-of-day) same day settlement (i.e. T+0) is still not a realistic near-term policy option as it would require a much more fundamental overhaul of the capital markets, FX/payments and securities

1 The March 2024 report of the UK's Accelerated Settlement Taskforce is available at https://www.gov.uk/government/publications/accelerated-settlement-taskforce.

2 See https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_24_422.

3 See, in this respect, Recommendation 3 in Annex C to the CPMI-IOSCO PFMI (available at https://www.bis.org/cpmi/info_pfmi.htm), derived from the 2001 Recommendations for Securities Settlement Systems which remain in effect today.

services processes. The move to a T+1 settlement cycle will require substantial system improvements, mainly by market participants rather than FMIs, to avoid increased settlement fails. Replacement cost risk may not diminish as anticipated due to a reduction in liquidity risk that is less substantial than expected. As regards overall implementation, careful planning and monitoring by the industry, regulators and supervisors will be required.

Editorial Committee

Annexes

Annex 1: Regulatory framework

FMIs	**FMIs CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs) (April 2012):** International standards for payment systems (PS), central securities depositories (CSDs), securities settlement systems (SSSs) and central counterparties (CCPs). They also incorporate additional guidance for over-the-counter (OTC) derivatives CCPs and trade repositories (TRs). https://www.bis.org/cpmi/publ/d101a.pdf
	CPMI-IOSCO Principles for Financial Market Infrastructures, Disclosure framework and assessment methodology (December 2012): Framework prescribing the form and content of the disclosures expected of FMIs; the assessment methodology provides guidance to assessors for evaluating observance of the principles and responsibilities set forth in the PFMI. https://www.bis.org/cpmi/publ/d106.pdf
	CPMI-IOSCO Recovery of financial market infrastructures (October 2014): Guidance for FMIs and authorities on the development of comprehensive and effective recovery plans. https://www.bis.org/cpmi/publ/d121.pdf
	CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (June 2016): FMIs are required to instil a culture of cyber risk awareness and to demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation. https://www.bis.org/cpmi/publ/d146.pdf
	ECB Cyber Resilience Oversight Expectations for FMIs (CROE, December 2018): The CROE aim to provide overseers with a clear framework with which to assess the cyber resilience of systems under their responsibility and to enable FMIs to enhance their cyber resilience. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
	Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0858

FMIs	**Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (14 December 2022).** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554
CCPs	**European Market Infrastructure Regulation (EMIR):** Regulation (EU) No 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs: EMIR sets a clearing obligation for standardised OTC derivatives and strict CCP risk management requirements, and requires the recognition and ongoing supervision of CCPs. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN
	EMIR Refit: Regulation (EU) 2019/834 of 20 May 2019: Mainly simplifies the derivative reporting and clearing obligation requirements, but also requires CCPs to provide information on their initial margin models, including simulation tools, to their clearing members. Further, the European Commission is empowered to suspend the clearing obligation for selected derivatives contracts, e.g. when markets are disrupted. https://eur-lex.europa.eu/eli/reg/2019/834/oj
	EMIR 2.2: Regulation (EU) 2019/2099 of 23 October 2019: This regulation improves the consistency of supervisory arrangements for CCPs established in the EU and enhances the EU's ability to monitor, identify and mitigate third-country CCP risks. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R2099
	CPMI-IOSCO Public quantitative disclosure standards for CCPs (February 2015): These standards complement the disclosure framework published by CPMI-IOSCO in December 2012. https://www.bis.org/cpmi/publ/d125.pdf
	EMIR Regulatory Technical Standards (August 2015): Regulation (EU) 2015/2205 of 6 August 2015 supplementing Regulation (EU) No 648/2012 with regard to regulatory technical standards on the clearing obligation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2205&from=EN
	CPMI-IOSCO Resilience of CCPs: Further guidance on the PFMI (July 2017): Guidance providing further clarity and granularity on several key aspects of the PFMI to further improve CCP resilience. https://www.bis.org/cpmi/publ/d163.pdf
	Regulation on CCP recovery and resolution: Regulation (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No 1095/2010, (EU) No 648/2012, (EU) No 600/2014, (EU) No 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2021:022:TOC

CSDs	**CSD Regulation (CSDR):** Regulation (EU) No 909/2014 of 23 July 2014 on improving securities settlement in the EU and on CSDs and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012: Prudential requirements on the operation of (I)CSDs as well as specific prudential requirements for (I)CSDs and designated credit institutions offering banking-type ancillary services. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en
	Regulation (EU) 2017/389 of 11 November 2016 supplementing Regulation (EU) No 909/2014 as regards the parameters for the calculation of cash penalties for settlement fails and the operations of CSDs in host Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0389&from=EN
	Regulation (EU) 2017/390 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on certain prudential requirements for CSDs and designated credit institutions offering banking-type ancillary services. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0390&from=EN
	Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for CSDs. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=EN
	Regulation (EU) 2023/2845 of the European Parliament and of the Council of 13 December 2023 amending Regulation (EU) No 909/2014 as regards settlement discipline, cross-border provision of services, supervisory cooperation, provision of banking-type ancillary services and requirements for third-country central securities depositories and amending Regulation (EU) No 236/2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302845&qid=1718611830620
Custodians	Regulation (EU) 2017/391 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards further specifying the content of the reporting on internalised settlements: Reporting obligation for settlement internalisers when settlement instructions are executed in their own books, outside securities settlement systems. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0391&from=EN
	Belgian Act of 31 July 2017: Act introducing a new category of credit institution carrying out activities exclusively in the area of custody, bookkeeping and settlement services in financial instruments, as well as non-banking services in relation thereto, in addition to receiving deposits or other repayable funds from the public and granting credit where such activities are ancillary or linked to the abovementioned services. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017073111&table_name=wet
	ESMA Guidelines on Internalised Settlement Reporting under Article 9 of CSDR (March 2018). https://www.esma.europa.eu/press-news/esma-news/esma-finalises-guidelines-how-report-internalised-settlement

Payment systems	**ECB Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (July 2014):** Regulation based on the CPMI-IOSCO PFMI, covering systemically important large-value and retail payment systems in the euro area. https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf
	Revised oversight framework for retail payment systems (RPS) (February 2016): Revised framework (replacing the 2003 version) identifying RPS categories and clarifying the oversight standards applicable to each. It also provides guidance on the organisation of oversight activities for systems of relevance to more than one central bank. https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf?bc332d9a718f5336b68bb904a68d29b0
PIs & ELMIs	**EMD2 (September 2009):** Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of ELMIs, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267, 10 October 2009, 7-17. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN
	PSD2 (November 2015): Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366
	Act of 11 March 2018 transposing PSD2, Moniteur belge/Belgisch Staatsblad of 26 March 2018. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018031107&table_name=wet/language=fr&la=F&cn=2018031107&table_name=loi
Payment processors	**Belgian Act of 24 March 2017 on the supervision of payment processors,** Moniteur belge/Belgisch Staatsblad of 24 April 2017. https://www.nbb.be/doc/cp/moniteur/2017/20170424_opp_wet_loi.pdf
	Royal Decree of 8 February 2019 on the requirements for processors of retail payment instruments and card payment schemes (CPS) having established a relationship with them on the due diligence that CPS must carry out when using the services of systemically relevant payment processors, the identification and management of risks by those processors, the continuity of their services and the practical arrangements for communication in the event of an incident. https://www.ejustice.just.fgov.be/eli/arrete/2019/01/25/2019030120/moniteur (FR) or https://www.ejustice.just.fgov.be/eli/besluit/2019/01/25/2019030120/staatsblad (NL)

Card payment schemes	European oversight framework for payment instruments, schemes and arrangements (PISA), November 2021. https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf
	Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions (OJ L 123, 19 May 2015, 1-15): This regulation defines (i) a ceiling for the interchange fees applicable to payment transactions by means of debit or credit cards, (ii) the separation to be ensured between payment card scheme governance activities and processing activities, and (iii) measures granting more autonomy to merchants regarding the choice of payment instruments for their clients. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN
	Belgian Act of 1 December 2016 transposing Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions (December 2016): Moniteur belge/Belgisch Staatsblad of 15 December 2016, 86.578. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2016120112&table_name=wet/language=fr&la=F&cn=2016120112&table_name=loi
	Regulation (EU) 2018/72 of 4 October 2017 supplementing Regulation (EU) 2015/751 on interchange fees for card-based payment transactions with regard to regulatory technical standards establishing the requirements to be complied with by payment card schemes and processing entities to ensure the application of independence requirements in terms of accounting, organisation and decision-making process, OJ L 13, 18 January 2018, 1-7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0072&rid=3
Swift	**High-level Expectations (HLE) for the oversight of Swift (June 2007):** The Cooperative Oversight Group has developed a specific set of principles applicable to Swift. https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers#oversight-of-swift-
	PFMIs, Annex F: Oversight expectations applicable to critical service providers (April 2012): Expectations for critical service providers of FMIs in order to support the overall safety and efficiency of FMIs. https://www.bis.org/cpmi/publ/d101a.pdf
	Assessment methodology for the oversight expectations applicable to critical service providers (December 2014): Assessment methodology and guidance for regulators, supervisors, and overseers in assessing critical service providers of FMIs against the oversight expectations in Annex F. https://www.bis.org/cpmi/publ/d123.pdf

Annex 2: FMIs established in Belgium with an international dimension

Euroclear

Euroclear Holding SA/NV, the top financial holding company of Euroclear, is incorporated under Belgian law. Euroclear Holding SA/NV owns 100% of Euroclear AG, a Swiss financial holding company. Euroclear Investments SA, a Belgian financial holding company, is an investment vehicle.

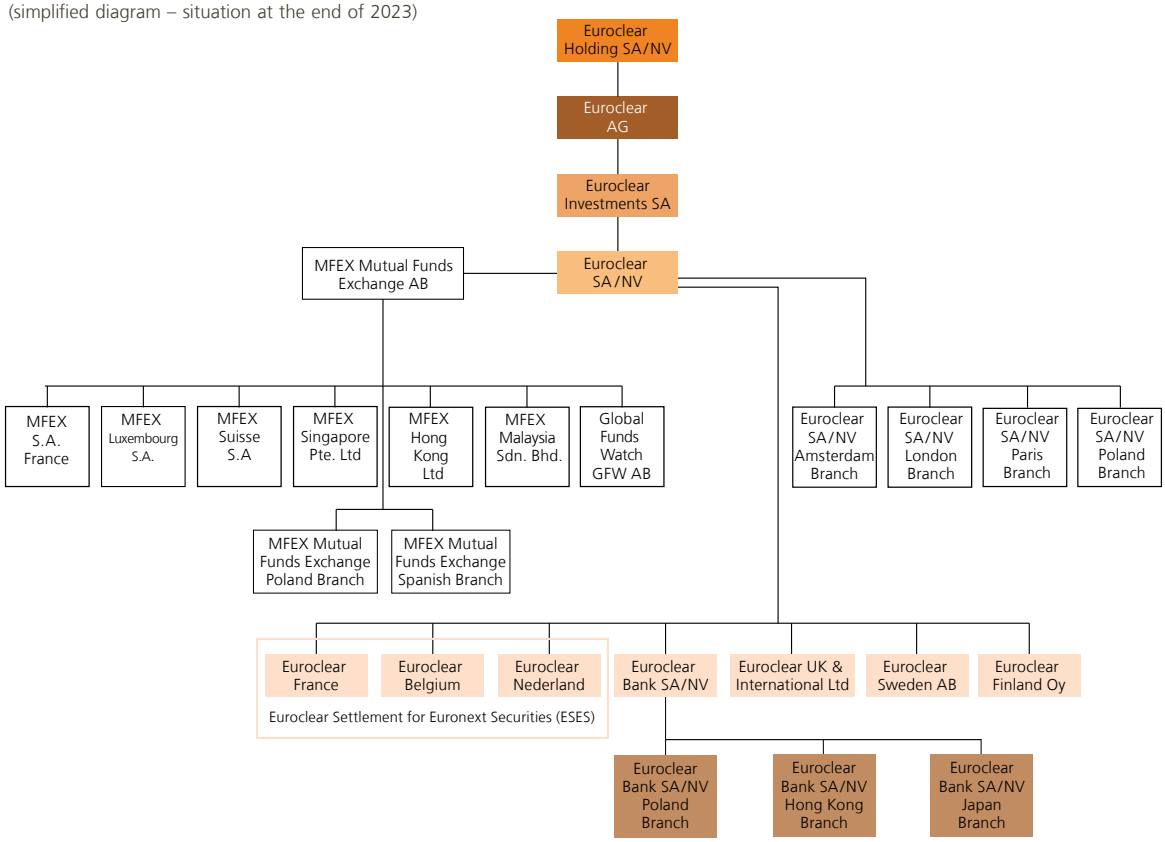
Euroclear SA/NV (ESA), also a Belgian financial holding company with branches in the Netherlands, the UK, France and Poland, is the parent company of the Euroclear Group (I)CSDs, i.e. the three ESES CSDs (Euroclear France, Euroclear Nederland, Euroclear Belgium), Euroclear UK & International Ltd, Euroclear Sweden AB, Euroclear Finland Oy and Euroclear Bank SA/NV. It owns the group's shared securities processing platforms and delivers a range of services to the group's depositories.

Euroclear Bank SA/NV, the ICSD of the group, has branches in Poland, Hong Kong and Japan.

Figure 1

Structure of the Euroclear group

(simplified diagram – situation at the end of 2023)



Source: Euroclear.

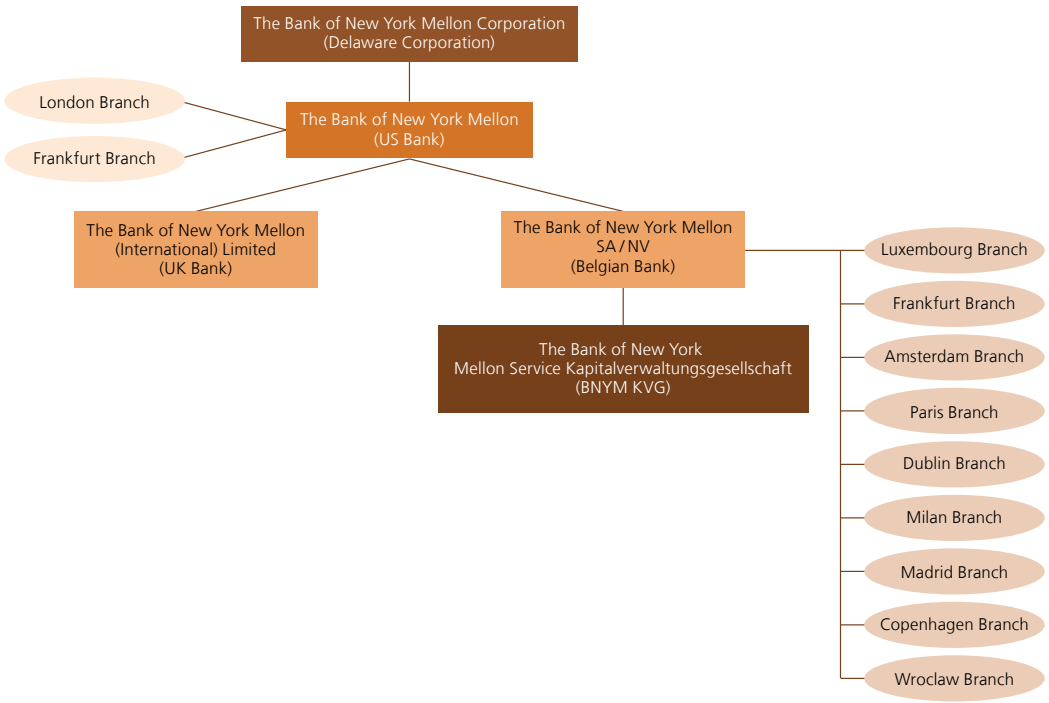
The Bank of New York Mellon

The Bank of New York Mellon SA/NV (BNYM SA/NV), established in Belgium, is the European subsidiary of BNY Mellon, a US-based global systemic bank, which in turn is a subsidiary of the US holding company BNY Mellon Corporation. BNYM SA/NV is the group's custodian bank for European clients and its gateway to euro area markets and payment infrastructures. BNYM SA/NV has a subsidiary in Germany and branches in Luxembourg, Germany, the Netherlands, France, Ireland, Italy, Spain, Denmark and Poland through which it operates on these markets. This structure is the result of the BNYM group's strategy to consolidate its operations in accordance with the so-called "Three Bank Model" (i.e. in the US/UK/EU).

Figure 2

Group structure of BNYM and position of BNYM SA/NV

(simplified diagram, situation at the end of 2023)



Source: BNY Mellon.

Worldline

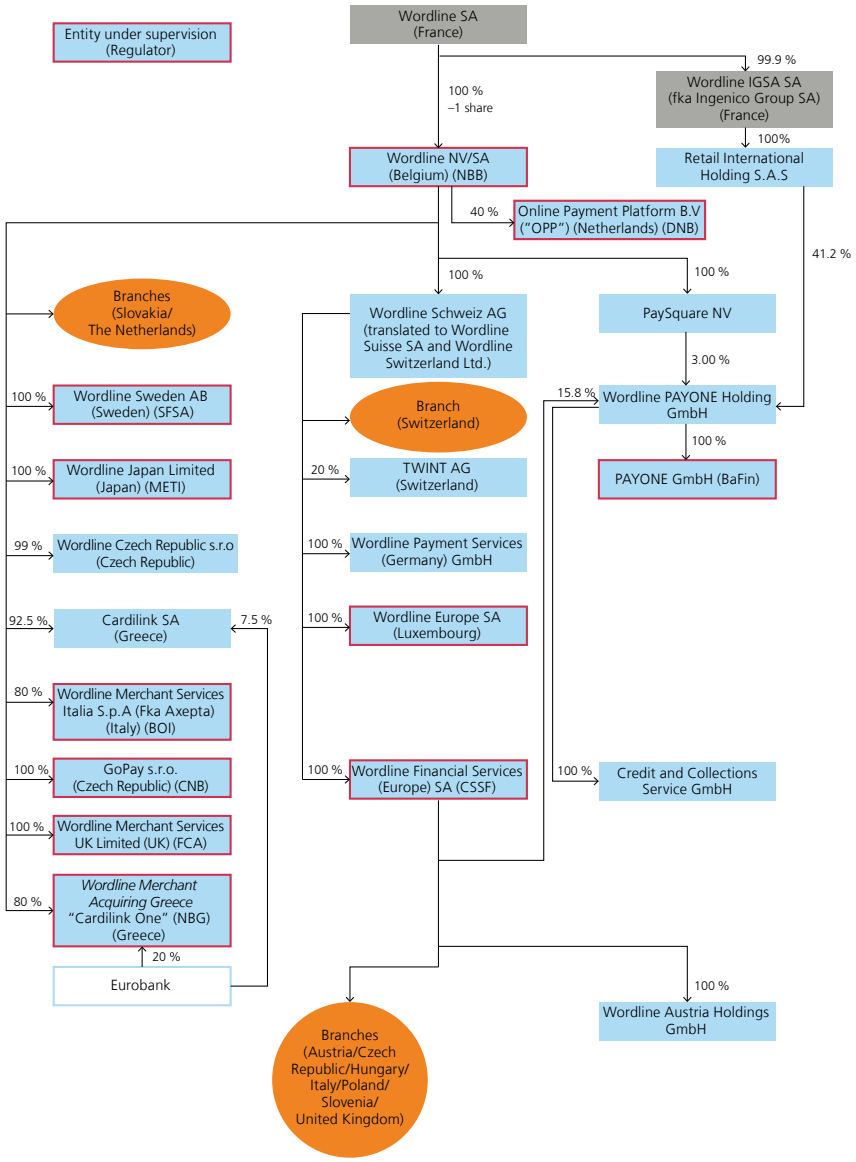
Worldline is a French group providing electronic payment and transaction services in Europe and beyond. In 2016, Worldline SA/NV, the group's Belgian entity, merged with the Dutch company Equens. The processing activities were carved out and placed in a new entity called equensWorldline SE. equensWorldline SE is now a wholly owned subsidiary of Worldline SA (France).

In 2018, Worldline acquired Six Payment Services, the payment division of the Swiss company SIX, which is now the main shareholder of Worldline SA (France). Since 2019, more than 75 % of Worldline's outstanding shares have been publicly held (free float). Following the acquisition of Ingenico, Worldline became the largest European provider of payment services.

Figure 3

Structure of Worldline

Simplified diagram, part of the group relevant for Belgium, as of 31 December 2023



Source: Worldline.

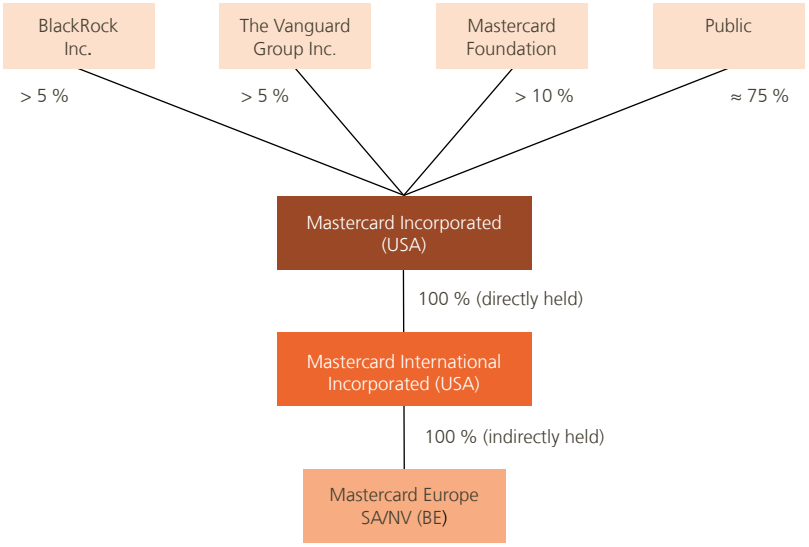
Mastercard Europe

Mastercard is a globally active payment services company. Mastercard Europe SA/NV (MCE), incorporated in Belgium, is a subsidiary of Mastercard Incorporated (listed on the New York Stock Exchange) and runs the company's business in Europe.

Figure 4

Mastercard group Structure

(simplified diagram, as of January 2023)



Source : Mastercard Europe.

Annex 3: Statistics

List of tables

Table 1

Securities settlement and custody statistics

(annual total in € billion equivalent, unless otherwise stated)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
A. Euroclear Bank										
Value of securities deposits (end of period)	11 765.3	12 393.7	12 698.4	12 834.2	13 451.5	14.823.6	15.292.4	17.105.3	17 528.3	18 293.7
Number of transactions (in millions)	75.2	83.3	84.1	95.4	107.0	116.4	128.8	146.9	163.3	170.8
Value of transactions	394 569.3	442 563.0	451 698.3	498 181.0	525 692.4	544.564.8	575.991.9	652.617.0	692 212.8	727 741.1
Source : Euroclear.										
B. NBB-SSS										
Value of securities deposits (end of period)	557.3	575.4	612.5	625.3	632.6	646.65	698.66	727.1	772.1	839.5
Number of transactions (in millions)	0.6	0.5	0.5	0.5	0.5	0.5	0.5	0.6	0.6	0.7
Value of transactions [1]	8 209.0	8 766.5	8 714.5	9 069.8	11 043.7	8 512.6	9 057.7	11 543.3	11 599.2	12 628.0
Source : NBB. 1 secondary market turnover.										
C. Euroclear Belgium										
Value of securities deposits (end of period)	222.1	269.4	235.1	237.7	178.0	220.2	194.9	218.9	193.3	194.8
Number of transactions (in millions)	2.1	2.5	2.4	2.5	2.7	2.6	2.9	2.7	2.6	2.4
Value of transactions	714.8	944.6	963.8	946.0	964.1	783.9	704.9	722.4	735.1	686.8
Source : Euroclear.										
D. TARGET2-Securities [1]										
Number of transactions (in millions)	nap	7.6	36.3	125.6	145.9	154.8	176.7	187.4	181.9	177.8
Value of transactions	nap	43 706.8	112 066.0	192 175.0	236 050.8	282 063.7	172 840.9	178 304.1	184 184.5	200 746.6
Source : ECB. T2S was launched in 2015. 1 The data in this table exclude technical transactions in T2S and liquidity transfers from traffic statistics as of 2020.										
E. BNYM SA/NV										
Value of assets held under custody (end of period)	3 454.0	3 216.4	3 476.5	3 608.8	2 373.1	2 873.5	2 903.5	3 290.4	2 834.4	3 105.1
Source : BNYM.										

Table 2

Payments

(annual total in € billion equivalent, unless otherwise stated)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
A. TARGET2										
Value of payments	498 726.5	508 982.3	485 811.8	432 780.7	432 508.1	441 281.1	465 793.7	484 251.6	570 539.0	494 492.9
of which: TARGET2-BE	16 247.9	15 627.4	16 957.9	19 732.4	22 594.7	24 935.5	28 570.6	27 921.2	29 411.7	32 119.1
Number of payments (in millions)	87.8	88.6	89.0	89.3	88.4	87.8	88.7	96.4	102.6	103.1
of which: TARGET2-BE	2.5	2.3	2.2	2.3	2.3	2.6	3.1	3.3	3.3	3.4
Source: ECB Payment Statistics. RTGS related payments, excluding TARGET2 transactions on dedicated cash accounts. Last year's figures are available at https://www.ecb.europa.eu/stats/payment_statistics/large_value_payment_systems/html/index.en.html.										
B. CLS										
Value of payments (in € trillion)	1 042 062.3	1 118 933.9	1 162 359.8	1 193 728.3	1 282 149.3	1 362 882.2	1 335 152.0	1 361 618.0	1 597 910.9	1 595 193.8
of which: EUR payments	191 170.5	208 555.8	204 370.7	219 924.6	241 067.1	249 090.1	244 744.0	254 388.0	292 542.1	284 034.2
Number of payments (in millions)	204.7	219.1	209.5	198.5	226.6	257.1	273.5	252.7	301.0	298.6
of which: EUR payments	34.4	40.9	34.3	34.0	39.1	42.2	45.4	41.2	50.8	47.5
Source: CLS.										
C. Centre for Exchange and Clearing (CEC)										
Value of payments (excluding instant payments since 2020)[1] (in € billion)	870.7	883.4	920.6	941.8	1 122.9	1 204.7	1 198.8	1 309.2	1 394.0	1 469.0
Value of instant payments (in € billion)	nap	nap	nap	nap	nap	nap	57.2	75.1	82.8	101.2
Number of payments (excluding instant payments since 2020)[1] (in millions)	1 272.2	1 402.2	1 387.1	1 312.0	1 456.7	1 512.7	1 396.9	1 467.8	1 395.0	1 473.5
Number of instant payments (in millions)							99.6	125.2	148.0	171.3
Sources: ECB, CEC. 1 Since 2020, data on instant payments have been reported separately.										

Table 2 (continued 1)

Payments

(end of period, total number, unless otherwise stated)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
D. Payment Institutions (PIs) – Electronic Money Institutions (ELMIs)										
PIs										
Belgian PIs	15	17	21	24	22	26	30	30	29	27
Account information service providers						1	3	4	6	6
Foreign PIs with a Belgian branch	3	3	3	2	3	4	5	6	7	9
Passport notifications for cross-border services of foreign EEA PIs towards Belgium	262	273	379	421	435	511	566	276 [1]	307	334
ELMIs										
Belgian ELMIs	10	10	8	8	7	7	7	6	5	5
Foreign ELMIs with a Belgian branch	1	1	1	1	2	1	1	1	1	1
Passport notifications for cross-border services of foreign EEA ELMIs towards Belgium	54	53	102	156	188	240	278	162 [1]	183	205
Institutions offering services within a limited network (new under PSD2)					1	4	5	5	9	12
Transactions by Belgian PIs and ELMIs (in millions)										
Number of transactions (yearly total)	1 874	1 968	2 155	2 006	2 044	1 949	2 106	2 358	2 595	3 068
Value of transactions in euro (yearly total)	133 513	136 567	137 144	124 388	124 485	113 639	121 751	177 792	202 155	257 734
Average outstanding e-money of Belgian ELMIs	21.8	35.8	45.5	73.9	116.6	405.2	494.3	481.7	302.8	314.8
Number of money remittances (yearly total, in millions)						5.7	11.2	31.0	48.5	nav
Value of money remittances (in millions)						1 546	3 043	17 304	19 903	nav
E. Processors of payment transactions										
Worldline SA/NV										
Number of transactions (yearly total, in millions) [1]	1 665.8	1 800.0	1 960.0	2 150.0 1 746	1 774	1 940	1 972	2 310	2 708	nav

Source : NBB.

1 Decrease due to Brexit.

Source : Worldline.

1 Owing to the transfer of some processing activities to equensWorldline SE, the volumes reported in this table as from 2017 refer only to the acquiring activities of Worldline SA/NV.

Table 2 (continued 2)

Payments

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
F. Card transactions										
Number of cards issued by resident payment service providers – cards with a cash function										
Number of cards (in thousands, end of period)	21 396.5	21 875.0	22 593.1	22 537.8	23 904.7	35 179.2	41 243.9	42 640.8	44 241.5	nav
Number of cards per capita (end of period)	1.9	1.9	2.0	2.0	2.1	3.1	3.6	3.7	4.3	nav
Transactions per capita										
Number of card payments – With cards isssued by resident PSPs [1] (yearly total)	135.2	130.9	149.5	158.5	183.0	202.3	213.0	238.7	271.6	nav
Value of card payments – With cards issued by resident PSPs [1] (yearly total, in € thousands)	7.2	7.4	8.1	8.2	8.5	9.1	9.3	10.3	11.6	nav

Source : ECB Payment Statistics.

1 Except cards with an e-money function.

G. Card schemes										
Bancontact – Number of transactions (yearly total, in millions)	1 241.8	1 306.7	1 389.5	1 441.6	1 480.2	1 593.4	1 706.1	1 982.2	2 270.3	2 419.7
of which :										
Payments	1 125.9	1 190.9	1 272.8	1 325.2	1 336.0	1 488.8	1 637.5	1 910.2	2 187.9	2 285.1
ATM [1]	115.9	115.9	116.8	116.3	114.2	104.6	68.6	72.2	146.8	134.6

Source : Bancontact.

1 Until 2021, figures on ATM withdrawals reported by Bancontact did not include “on-us” operations (i.e. withdrawals made at an ATM operated by the issuer of the card used). Since 2022, on-us withdrawals of KBC, ING, BNP Paribas Fortis and Belfius made at ATMs operated by Batopin (their common ATM network provider) have been included in the figures.

Table 3

Swift statistics

(yearly total, in millions)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Number of messages	5 612.7	6 106.6	6 525.8	7 076.5	7 873.6	8 454.4	9 526.5	10 593.7	11 254.9	11 949.5
of which:										
Payment messages	2 737.2	2 930.2	3 139.3	3 485.2	3 840.0	4 053.4	4 313.0	4 799.5	4 992.8	5 257.8
Securities messages	2 545.2	2 829.1	3 019.1	3 232.3	3 635.5	3 968.9	4 709.8	5 269.2	5 714.8	6 094.2
Other messages	330.3	347.3	367.3	359.0	398.1	432.1	503.8	525.0	547.3	597.5

Source: Swift.

List of abbreviations

AFM	Autoriteit Financiële Markten
AFME	Association for Financial Markets in Europe
AIFMD	Alternative Investment Fund Managers Directive
AMF	Autorité des marchés financiers
API	Application programming interface
APT	Advanced persistent threat
ART	Asset-referenced token
ATM	Automated teller machine
BdF	Banque de France
BCBS	Basel Committee on Banking Supervision
BCL	Banque Centrale de Luxembourg
BIC	Bank Identifier Code
BNYM	Bank of New York Mellon
BoE	Bank of England
BoJ	Bank of Japan
CASP	Crypto-asset service provider
CBDC	Central bank digital currency
CBPR+	Cross-border payments and reporting
CCP	Central counterparty
CCP-RRR	CCP Recovery & Resolution Regulation
CEC	Centre for Exchange and Clearing
CER	Critical Entities Resilience Directive
CET1	Common Equity Tier 1
CHAPS	Clearing House Automated Payment System
CHF	Swiss franc
CHIPS	Clearing House Interbank Payments System
CLS	Continuous Linked Settlement
CPMI	Committee on Payments and Market Infrastructures
CPS	Card payment scheme
CRD	Capital Requirements Directive
CROE	Cyber Resilience Oversight Expectations for FMIs
CRR	Capital Requirements Regulation
CSCF	Customer Security Controls Framework
CSD	Central Securities Depository
CSDR	Central Securities Depository Regulation
CSP	Customer Security Programme
CSPAC	Customer Security Programme Assessor Certification
CSSP	Commission de Surveillance du Secteur Financier
CTPP	Critical ICT third-party service provider

DE	Germany
DLT	Distributed ledger technology
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
DTCC	Depository Trust and Clearing Corporation
DVP	Delivery versus payment
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EEA	European Economic Area
EG	Executive Group
ELMI	Electronic money institution
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
EMT	Electronic money token
ENISA	European Union Agency on Cybersecurity
ESA	Euroclear SA/NV
ESAs	European supervisory authorities (EBA, ESMA and EIOPA)
ESAS	New Zealand's Exchange Settlement Account System
ESCB	European System of Central Banks
ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
ESG	Environmental, social and governance
EU	European Union
FMI	Financial market infrastructure
FR	France
FSB	Financial Stability Board
FSMA	Financial Services and Markets Authority
FX	Foreign exchange
G7	Group of Seven
G10	Group of Ten
G20	Group of 20
GPI	Global Payments Initiative
G-SIB	Global systemically important bank
HLE	High-level expectation
HU	Hungary
IAF	Independent Assessment Framework
IBAN	International Bank Account Number
ICE	Intercontinental Exchange
ICSD	International central securities depository
ICT	Information and communication technology
IOSCO	International Organisation of Securities Commissions
IRRBB	Interest rate risk in the banking book
ISAC	Information Sharing and Analysis Centre
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IMF	International Monetary Fund

JST	Joint Supervisory Team
KPI	Key performance indicator
KRI	Key risk indicator
KYC	Know your customer
KYS	Know your supervisor
LCH	London Clearing House
LVPS	Large-value payment systems
MCE	Mastercard Europe
MCMS	Mastercard Clearing Management System
MiCA	Markets in crypto-assets
MoU	Memorandum of understanding
NBB	National Bank of Belgium
NCA	National competent authority
NCB	National central bank
NFC	Near field communication
NIS	Network and information security
NL	The Netherlands
NSD	National Securities Depository
NV	Naamloze vennootschap
OC	Oversight committee
OG	Oversight Group
O-SII	Other systemically important institution
OSR	On-site review
OTC	Over the counter
PFMI	CPMI-IOSCO Principles for FMIs
PI	Payment institution
PIRPS	Prominently important retail payment system
PISA	Payment instruments, schemes and arrangements
PMO	Payments Market Infrastructure
PMPG	Payments Market Practice Group
PSD	Payment Services Directive
PSP	Payment service provider
PSR	Payment Services Regulation
PVP	Payment versus payment
REFIT	Regulatory fitness and performance
RITS	Reserve Bank of Australia Information and Transfer System
RPS	Retail payment system
RTGS	Real-time gross settlement
RWA	Risk-weighted assets
SA	Société anonyme
SCA	Strong customer authentication
SCT	SEPA credit transfer
SDLC	Software development lifecycle

SE	Societas Europaea
SEPA	Single European Payments Area
SIPS	Systemically important payment system
SOF	Swift Oversight Forum
SREP	Supervisory Review and Evaluation Process
SSM	Single supervisory mechanism
SSS	Securities settlement system
Swift	Society for Worldwide Interbank Financial Telecommunication
T2S	TARGET2-Securities
T	Trade data
TIBER	Threat intelligence-based ethical red teaming
TG	Technical Group
TLPT	Threat-led penetration testing
TM	Transaction Manager
TPRM	Third-party risk management
UCITS	Undertakings for collective investment in transferable securities
US	United States

National Bank of Belgium
Limited liability company
RLP Brussels – Company number: 0203.201.340
Registered office: boulevard de Berlaimont 14 – BE-1000 Brussels
www.nbb.be

Publisher

Tim Hermans
Executive Director

National Bank of Belgium
Boulevard de Berlaimont 14 – BE-1000 Brussels

Contact for the publication

Dominik Smoniewski
Head of
Surveillance of financial market infrastructures, payment services and cyber risks

Tel. +32 2 221 20 57
dominik.smoniewski@nbb.be

Cover and layout: NBB CM – Prepress & Image

Published in June 2024