Overview of the NBB's oversight and supervision of financial market infrastructures in 2013

The Bank is responsible not only for the oversight but also for the prudential supervision of post-trade financial market infrastructures (FMIs). The central bank's oversight promotes the safety and efficiency of the payment and settlement infrastructures, and ultimately of the financial system as a whole. The prudential supervision ensures the robustness of the market infrastructures' operator at micro-level, thus helping to maintain the confidence of the institution's counterparties. Within the Bank, the two functions are performed by the same entity.

Table 1 contains an overview of the (cooperative) oversight and/or supervision of FMIs in which the NBB is involved. Many of the infrastructures that are overseen and/or supervised by the NBB have an international dimension; some of them limit their operations to the euro area, others operate worldwide. In line with the principles for cooperative oversight and supervision, the NBB performs the role of lead overseer/supervisor for international infrastructures established in Belgium, such as SWIFT and Euroclear. As a corollary, and under the leadership of the relevant national central bank/supervisor, the NBB plays a role in cooperative oversight and supervision for international infrastructures established outside Belgium, but providing services to Belgium.

1. Oversight and supervision of securities settlement systems and operators

The Bank acts as the overseer of securities settlement systems, and as a prudential supervisor of their operator, with respect to three Euroclear group entities. In addition, it acts as the overseer of NBB-SSS (Securities Settlement System), operated by the NBB itself. Finally, the Bank has oversight and/or prudential supervision competencies in relation to the Bank of New York Mellon (BNYM) Group entities established in Belgium.

1.1 Oversight and supervision of Euroclear group

The Bank acts as an overseer and as a prudential supervisor of three Euroclear group entities: Euroclear SA/NV (ESA), Euroclear Bank (EB) and Euroclear Belgium.

ESA

ESA is the Euroclear group's parent company. It owns and manages the IT infrastructure and offers common support services to the (international) central securities depositories – (I)CSDs of the group. A framework has been set up organising co-ordination and cooperation between the twelve authorities of the countries of which an (I)CSD is consolidated into the Euroclear group. The Bank acts as coordinator for the purpose of this multilateral arrangement which organises the exchange of information and the coordinated assessment of the ESA common services. It encompasses issues relating inter alia to operational reliability, governance, and organisation of the audit and risk management functions, as well as the group's strategy.

In the past year specific attention was devoted to issues concerning cyber-defence and to the ESA recovery plan that will be further assessed in the light of the CPSS-IOSCO Guidance for Recovery of Financial Market

TABLE 1 FINANCIAL MARKET INFRASTRUCTURES SUBJECT TO THE BANK'S SUPERVISION AND OVERSIGHT

	Institutions / Systems covered		
	International supervisory college / Cooperative oversight arrangement		NBB solo authority
	NBB lead authority	NBB takes part, other authority is lead	
Prudential supervision	Bank of New York Mellon SA (BNYM)[3]		BNYM Brussels branch
			25 Payment & electronic money institutions
Prudential supervision & Oversight	Euroclear Belgium (formerly CIK) (ESES)	8 EU CCP colleges[4]	
	Euroclear SA/NV (ESA) Euroclear Bank – ICSD[1]		
			Bank of New York Mellon CSD
Oversight	SWIFT	Target2Securities (T2S)[2]	NBB-SSS
		Target2 (T2)[2]	Bancontact/Mister Cash[2]
		CLS	UCV/CEC[2]
			MasterCard Europe[2]

Securities clearing, settlement & custody
Payments and card schemes
Critical service providers to the financial infrastructure

(1) The NBB cooperates bilaterally with other relevant central banks (ECB, CBL, CBoI, BoJ) on an ad hoc basis. A multilateral MOU is under discussion.
(2) Peer review in Eurosystem/ESCB.
(3) Pre SSM situation – BNYM SA is the European Headquarter of the BNYM group. The NBB is lead authority of the college of European Supervisors and participates in the US College of the group supervisors, as well as in the FSB BNYM Crisis management group.
(4) LCH.Clearnet Ltd, LCH.Clearnet SA, Eurex Clearing AG, EuroCCP, KDPW_CCP, Keler CCP, CC&G, ICE Clear Europe.

Infrastructures which is to be issued in 2014. These recovery plans should enable ESA and each individual (I)CSD to cope with threats to their viability and financial strength and to continue to provide their critical services by relying on a variety of tools, depending on the potential stress scenario.

EUROCLEAR BANK

As an international central securities depository (ICSD), Euroclear Bank (EB) provides settlement and custody services for international securities (eurobonds), domestic bonds, equities and fund instruments. It has established

a network of more than 40 links with domestic markets worldwide and provides its services to more than 1 400 participants.

As the lead overseer of EB, the Bank monitored the measures taken by EB to further reduce the liquidity risk which is basically of an intraday nature and originates from the credit extended by EB to its participants to support and facilitate the settlement process. Even if fully collateralised, such credit operations could typically expose EB to liquidity pressure, should the participant with the largest exposure default. Structural measures have been further implemented by EB in order, on the one hand, to reduce the level of its credit activity and, on the other, to enlarge its access to committed liquidity sources in contingency situations. In March 2013, EB implemented system changes to optimise the settlement of short-term triparty repo roll-overs. Thanks to the synchronisation of triparty initiations and closings, the provision of intraday credit by EB has declined significantly. Further initiatives are under review to reduce the intraday credit activities, inter alia by further optimising the current settlement processes. Overall, the liquidity risk management framework has been significantly enhanced in recent years. The new challenges that could arise from strategic developments in the Euroclear business model and in its environment will continue to be monitored by the NBB in order to ensure that such changes do not affect EB's overall liquidity risk profile.

The credit risk arising from its settlement processes is fully mitigated by EB through full collateralisation of exposures to participants. Regarding the asset servicing activities, EB was requested to adapt its current procedures and applicable credit risk management framework. According to the new procedure that will be implemented in the course of 2014, income and redemption proceeds will no longer be paid in advance to the participants before the related payment is received from the issuer. This will allow EB to comply fully with the applicable CPSS-IOSCO Principles.

In addition, the Bank reviewed EB's access criteria in order to take better account of the variety of profiles of its participants and to mitigate potential additional risks resulting from their participation in the system. Besides the standard access conditions applicable to participants that are credit institutions, investment firms or financial institutions supervised in the Union, specific requirements have been developed for participants that are supervised financial institutions established outside the Union and for non-regulated legal entities. These requirements cover financial resources, operational readiness, and legal capacity, as well as internal control and risk management. This review was initiated in conformity with the Belgian finality law, as updated in January 2013.

The new CPSS-IOSCO framework also outlines the general responsibilities of the relevant authorities for Financial Market Infrastructures in implementing the standards. Responsibility E, in particular, requires them to cooperate both domestically and internationally to support each other in fulfilling their respective mandates. For the oversight of EB, a multicurrency critical Financial Market Infrastructure, the Bank had already developed cooperative arrangements with national and foreign authorities, including the FSMA and the ECB. The Bank is currently discussing setting up bilateral and multilateral cooperative oversight arrangements with other central banks. In the context of the EU FSAP on pan-European critical market infrastructures, the IMF also recommended formalising and enhancing the existing cooperation between the Belgian and Luxembourg authorities regarding the link between EB and Clearstream Luxembourg, and involving the ECB in the updated arrangements. This aims at ensuring a level playing field in the effective and parallel implementation of the CPSS-IOSCO Principles by the two ICSDs.

From a banking supervisory perspective, specific attention was given to capital requirements issues and to compliance with the prudential requirements regarding the Large Exposure Regime and the concentration risk. Any adjustments to the strategy and business model are monitored by the Bank in order to reflect potential risk profile changes in the Supervisory Review and Evaluation Process and/or compliance with regulatory norms. Other actions concerned the assessment of significant model changes and compliance with European rules regarding remuneration policy.

From an event-driven and risk-based supervision perspective, the main actions concerned the monitoring of potential risk profile modifications of the Euroclear SA subsidiaries and Euroclear Bank branches resulting from the implementation of new technical and business projects, new activities and related organisational changes. That monitoring feeds into the ICAAP-SREP process and aims at ensuring that adequate risk management, functional and organisational changes and the adaptation of Internal Control Systems are implemented in order to ensure that the framework remains fit for purpose and effective on a continuous basis.

Finally, due attention was paid to on-going strategic developments and the responses provided by Euroclear Bank to changes concerning the market and regulation (e.g. CRD IV, EMIR, AIFMD, CSDR, CPSS-IOSCO Principles).

EUROCLEAR BELGIUM

Euroclear Belgium mainly holds Belgian securities, in particular Belgian equities. It settles participant transactions on the same platform "ESES" (Euroclear Settlement for Euronext zone Securities) as Euroclear France and Euroclear Nederland. The Bank continued its regular monitoring of the Euroclear Belgium CSD's functioning, including the development by Euroclear Belgium of new services for issuers. For common ESES aspects, there is coordinated supervision and oversight. The Bank – together with its Dutch and French equivalents and the securities commissions of the ESES countries – monitored the ESES CSDs' ongoing implementation of the T2S project.

1.2 Oversight of NBB-SSS

A complete assessment of NBB-SSS against the CPSS-IOSCO Principles for Financial Market Infrastructures (published in April 2012) has begun. The transition to a new platform ("Ramses") in preparation for TARGET2-Securities is also being monitored from an oversight perspective. In 2014, the monitoring of the testing phase will be one of the priorities.

1.3 Supervision and oversight of the Bank of New York Mellon group

PRUDENTIAL SUPERVISION OF THE BANK OF NEW YORK MELLON SA/NV (BNYM SA/NV)

After several years of mergers of the various BNYM group's European legal entities within BNYM SA/NV in order to transform these entities into branches as part of the strategic move towards a single European banking structure, 2013 brought further consolidation of the resulting structure of the SA.

The Bank closely monitored changes to BNYM SA/NV's governance and risk management framework in order to ensure that developments in these domains were commensurate with the geographical extension and enlargement of the activities of BNYM SA/NV.

The inclusion of new activities in the activity mix of BNYM SA/NV was also closely followed due to the specific constraints applicable, in that field, to "equivalent settlement institutions", a Belgian regulatory status for institutions providing services of significant importance to CSDs.

Similarly, the collaboration with the main regulators of the group was further strengthened through the organisation of the EEA College and participation in International Colleges (the BNYM FSB College and the Crisis Management group), as well as through bilateral cooperation.

BNYM SA/NV is one of the 130 Significant Banks included in the Single Supervisory Mechanism. Accordingly, the Bank has begun to prepare the transfer of supervisory responsibility for BNYM SA/NV to the ECB in line with the SSM methodology and planning. Those preparations will continue throughout 2014.

BNY MELLON CSD SA/NV

The Belgian-based BNY Mellon CSD SA/NV (a non-bank subsidiary of the BNYM Corporation) is overseen and supervised by the Bank.

In the course of 2013, BNYM CSD was officially notified as a system under the Settlement Finality Directive and its operational readiness was assessed. The gradual roll-out of its services will be reviewed by the Bank as prudential supervisor and overseer, in accordance with the applicable regulatory requirements.

2. Oversight and supervision of retail payment services

2.1 Contribution to standard setting : European Forum on the security of retail payment services

The European Forum on the Security of Retail Payment Services, under the aegis of the Eurosystem and the ESCB, brings together representatives of the EU authorities in charge of oversight and prudential supervision. It aims to facilitate common knowledge and understanding, between the authorities concerned, of the security issues linked to electronic/mobile retail payment instruments and other internet-based payment services offered within the EU.

In January 2013, the Forum published its first report devoted to the security of internet payments, and containing a set of recommendations for providers of services covered by the Payments Services Directive (PSD), and for payment scheme governance authorities that are responsible for the overall functioning of of the payment scheme.

The Forum also focused its activities on finalising its recommendations regarding the security of payment account access services (account information services and payment initiation services). The Forum was well supported, mainly by banking and payment associations, which participated in the public consultation from February to mid April 2013. The most crucial conclusion of this work stream, from a security point of view, relates to the necessity for third party providers (TPPs)[1] to ensure that customers are appropriately authenticated by relying on strong customer authentication, with no sharing with the TPP of the credentials granted to the customer by the account servicing payment service providers, i.e. the bank holding the customer's payment account.

Another main work stream of the Forum resulted in a proposal for "recommendations for the security of mobile payments" which was published for a public consultation that ran from November 2013 to January 2014. Three categories of mobile payments are distinguished, namely contactless payments (Bluetooth, NFC, etc.,) payments using a mobile payment application ("app"), and payments through mobile network operators' channels (sms, voice technology) without a specific "app" downloaded onto the mobile device.

The intended addressees of the recommendations, the mobile payment solution providers, include all payment service providers pertaining to the PSD perimeter when offering mobile payment services, as well as the governance authorities of payment instrument schemes which provide mobile payment services.

The final set of "recommendations for the security of mobile payments", as amended following the public consultation, is expected in the second half of 2014.

2.2 Prudential supervision of payment institutions and electronic money institutions

At the end of 2012 the second Electronic Money Directive was transposed into Belgian law. The new law also introduced conditions under which both e-money institutions and payment institutions could provide services under exemption waiver so that they are only subject to a "light" regime.

These "light" regimes enable smaller payment service and electronic money providers with a business volume below certain thresholds as defined in the law (for payment institutions: yearly turnover of € 36 million in payment services, for e-money institutions: an outstanding amount of € 5 million in e-money) to enter the market and to provide regulated services. In general, these institutions are exempted from most of the existing regulatory and reporting requirements. However, they remain subject to the legal obligation to appoint an external auditor to check their (limited) reporting requirements and compliance with the threshold, and to the obligation to submit a yearly anti money laundering report.

In 2013, the NBB granted authorisation to three payment institutions and three institutions for electronic money. Three service providers were licensed to start providing activities with waiver conditions as prescribed by law.

The number of non-banks providing payment services and electronic money services in Belgium is growing. By the end of 2013, 25 institutions were offering services, against 18 institutions at the end of 2012. Seven of those institutions are operating under waiver conditions (light regime) and two are branches of payment institutions located in other Member States of the European Union.

In 2013 the NBB started the assessment of the procedures in place at the payment institutions and e-money institutions to prevent money laundering and combat fraud and terrorist financing.

2.3 Oversight of retail payment systems

Since the end of March 2013, the Centre for Exchange and Clearing (CEC), the Belgian automated clearing house which processes and clears retail payments between banks active in Belgium, has been using the technical platform "CORE" of the French automated clearing house, the Systèmes Technologiques d'Echange et de Traitement. This migration was the occasion to improve the risk management of the system. Two major changes concerned the frequency of the settlement cycles, which was increased from one to five daily cycles, and the introduction of transaction messaging to the beneficiary's bank after final settlement takes place in the settlement system, Target2. These changes were made on the basis of the NBB's oversight recommendations.

Although the CEC uses the same technical infrastructure as its French equivalent, it remains a separate, legal Belgian entity. In the framework of its oversight activities,

(1) A third-party provider (TPP) accesses the payment account of a customer making a purchase on the internet or provides information about one or more accounts with one or more account servicing payment service providers.

the NBB paid specific attention to the preparation and implementation of the migration, which went off smoothly without any operational incident or service disruption.

2.4 Oversight of card payment schemes (CPS)

A comprehensive oversight assessment on MasterCard Europe (MCE) was concluded by the end of 2012. It was conducted by the Eurosystem assessment group and coordinated by the Bank ; the assessment report was compiled in the first half of 2013. This initiated the follow-up phase, encompassing, among other things, possible implementation of adequate mitigation measures to comply with the recommendations.

A Eurosystem public report providing a comprehensive view of the trends in the Card Payment Schemes sector is being prepared and is expected around mid-2014.

In May 2013, in the spirit of the prevailing international standards in the field of oversight, the Bank signed a memorandum of understanding with the Central Bank of Russia and MasterCard Europe determining the details surrounding the exchanges of information between the two authorities in the context of the Central Bank of Russia's competences vis-à-vis the MasterCard Europe subsidiary established in Russia.

The Bancontact-MisterCash debit card scheme continued its adaptation to comply with the Single Euro Payments Area (SEPA) principles. These principles imply that card schemes will become open for all issuers and acquirers throughout Europe, and that security for cards and terminals is based on internationally accepted standards (EMV)[1]. The necessary update of the scheme's infrastructure was completed in 2013. As the overseer of the scheme, the Bank monitored these developments, focusing on the financial risk management and on the scheme's new projects, including the Bancontact-MisterCash mobile payment application for which a one-year pilot phase was launched at the beginning of 2013.

3. Oversight of SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a critical service provider used to exchange standardised financial messages worldwide. Central bank oversight of SWIFT is justified because SWIFT provides these messaging services for correspondent banking activities and for critical Financial Market Infrastructures such as payment and securities settlement systems. SWIFT's security and availability are of crucial importance for the safety and efficiency of these Financial Market Infrastructures.

The NBB acts as lead overseer of SWIFT[2]. At SWIFT, the major risk category under review is operational risk. The oversight is performed in cooperation with the G10 central banks. Since 2012, information has been shared with a wider group of central banks, as the country representation in the SWIFT oversight arrangements was expanded with the establishment of the SWIFT Oversight Forum. In the Forum, senior representatives of the G10 and ten other central banks conduct joint discussions on the SWIFT oversight policy and results. The first meetings of the SWIFT Oversight Forum were held in 2012 and the cooperation and exchange of information with the SWIFT Oversight Forum central banks were further intensified in 2013.

In order to structure their oversight activities vis-à-vis SWIFT, the overseers translated their focus on SWIFT's management of operational risks into the drafting of five High Level Expectations (HLEs). The HLEs centre around security measured in terms of confidentiality, integrity, availability and system resilience. There are five HLEs that formulate expectations in the areas of Risk Identification and Management, Information Security, Reliability and Resilience, Technology Planning and the Communication with Users. The HLEs constitute the framework for reviewing SWIFT activities that fall within the scope of the oversight. The overseeing central banks address their common security and resilience expectations *directly* to SWIFT.

In 2013, SWIFT provided its overseers with an updated self-assessment report regarding its compliance with the HLEs. SWIFT's demonstration of compliance with the HLEs does not reflect the overseers' opinion, but SWIFT's own assessment of how it lives up to the HLEs.

To avoid the risk that different overseers may use different oversight/assessment frameworks to assess the functioning of critical service providers, thereby creating an unlevel playing field, CPSS and IOSCO in their Principles for Financial Market Infrastructures added "*Annex F: Oversight expectations applicable to critical service providers*", which suggests an oversight approach for other critical service providers that is similar to what the overseers of SWIFT aim to achieve with the HLEs. In December 2013, CPSS and IOSCO issued an *Assessment methodology for the oversight expectations applicable to*

(1) EMV: Europay MasterCard Visa is the international standardised protocol for Chip and PIN security for card payment transactions.

(2) A detailed description of the set-up of the international co-operative oversight of SWIFT was provided in the 2013 issue of the NBB's Financial Stability Review, pp. 120-122.

critical service providers. CPSS and IOSCO invited industry comments on this consultative report. This CPSS-IOSCO assessment provides guidance for authorities in assessing an FMI's critical service providers against the oversight expectations in Annex F, and at the same time provides guidance for critical service providers on compliance with the oversight expectations.

Two major SWIFT projects reviewed by the overseers in 2013 were "Distributed Architecture" and "FIN Renewal". Both projects are multi-year platform investments that help to increase the security, resilience and reliability of the services provided. The Distributed Architecture set up a multi-zonal messaging architecture, allocating countries to either the European or the Trans-Atlantic zone. As opposed to the processing of messages that are being sent between customers in different zones, messages between customers within the same zone are only processed in that zone. The Distributed Architecture project added a SWIFT operating centre for the European zone as well as an additional command and control capability in Asia, enabling operations to be controlled from either Asia, Europe or the US. Operational improvements are made at every SWIFT operational site, and include the renovation of computer rooms and the power and cooling infrastructures. The latest major initiative was the construction of a new state-of-the-art operating centre that replaces one of those currently in use. Operations were successfully transferred to the new operating centre in 2013. Monitoring the progress of this building project was a major focus of overseers in 2013. Some final project deliverables are scheduled for 2014.

The second major SWIFT project reviewed by overseers is the FIN renewal project. The underlying technology platform of FIN, SWIFT's core application for messaging, is being renewed to address long-term technology needs (e.g. to avoid technology obsolescence or increase flexibility in line with technological progress) while aiming to significantly reduce ongoing operating costs. The scope of this project is only to adapt the central FIN application, not the FIN interfaces and SWIFT network connections at the customers' end. The first components of the renewed application were successfully launched in 2013. The second and third stages of the FIN renewal project extend into the years to come. Aspects reviewed include risk management, project management including the monitoring of project milestones, test strategies, and transparency of communication in relation to vendors and customers.

Overseers in 2013 further increased their monitoring of cyber security initiatives at SWIFT. The logical security protection of the SWIFT operations is continuously reassessed and drives management decisions to strengthen protection, in line with the industry-wide observations that cyber security threats are on the rise.

Standing topics for review by overseers include IT audit reports, technology and information, security risk management, and the development of an enterprise-wide risk management framework. Furthermore, overseers continue to monitor closely SWIFT's financial position, as well as trends in its messaging volumes. SWIFT's FIN messaging traffic is the major contributor to the company's revenue and increased above budget in 2013. SWIFT's Chief Risk Officer (CRO) in 2013 continued the development of an integrated Enterprise Risk Management framework throughout SWIFT. In 2013, overseers conducted a major review of the set-up and functioning of SWIFT's governance arrangements. Governance is the set of relationships between SWIFT's cooperative shareholders, board of directors, management, and other relevant parties, including its users, authorities, and other stakeholders (such as users' customers, interdependent FMIs, and the broader market). Governance provides the processes through which the organisation sets its objectives, determines the means for achieving those objectives, and monitors performance against those objectives. Good governance provides the proper incentives for an FMI's board and management to pursue objectives that are in the interest of its stakeholders and that support relevant public interest considerations. As the conclusions of the SWIFT governance review were positive, any new review of SWIFT governance arrangements by overseers would be triggered by changed requirements based on evolving international best practices, governance changes made by SWIFT, issues revealed under the current arrangements, or the need to update the current assessment from time to time.