G. Cross-sectoral aspects of prudential regulation and supervision

As a prudential supervisory authority, the Bank is competent for a range of spheres which cover multiple sectors and are therefore not discussed in the sections of this Annual Report on banking, insurance and financial market infrastructures.

In 2017, one of the main developments was the completion of the work on transposing into Belgian law the Fourth EU Directive on the prevention of money-laundering and terrorist financing, which will demand a major effort on the part of both financial institutions and the competent authorities, including the Bank.

The Quality Assurance Unit, intended to ensure that the Bank's prudential supervision and resolution activities satisfy a number of quality requirements, continued working on the definition of its framework in order to progress gradually towards a definitive method of operation.

During the year under review, the Bank also set up a single point of contact for FinTech, in collaboration with the FSMA, which acts as the supervisory authority's access channel for questions concerning the legislative framework for the provision of financial services in Belgium, notably in the context of the European Payment Services Directive (PSD2). The Bank also kept a close watch on developments relating to private digital currencies.

In view of the growing cyber threats, the Bank actively contributed to the further development, at European level, of a regulatory framework for the management of cyber risks and recommendations on the subject. During the year under review, it also carried out a number of inspection assignments concerning cyber risk. Finally, in collaboration with other players, the Bank continued its work aimed at mapping e-banking fraud and raising consumers' awareness of the issue.

As regards governance, reporting and the collaboration of auditors in prudential supervision, the year under review brought the adoption and publication by the Bank of several new normative documents on such matters as the quality of prudential and financial data, the cooperation of accredited auditors in prudential supervision, reporting on loans to related persons, qualifying holdings, the "fit and proper" framework and the compliance function.

1. Measures to combat money-laundering and terrorist financing

The year 2017 brought the final touches to the work on transposing into Belgian law – via the Law of 18 September 2017 [1] – the Fourth EU Directive on the prevention of money-laundering and terrorist financing (ML/TF) [2]. This new Law makes a transition to mechanisms resolutely aimed at the general adoption of a risk-based approach, as regards both the preventive obligations of financial institutions and the supervision by the competent authorities, including the Bank, over compliance with those obligations. This development requires both parties to make significant efforts to adapt the arrangements that they had defined and implemented under the previous Law.

(1) Law of 18 September 2017 on the prevention of money-laundering and terrorist financing and limits on the use of cash.

(2) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

1.1 Law of 18 September 2017

The structure of the new Law was radically revised compared to that of the Law of 11 January 1993, which it abolishes and replaces. In particular, all the obligations imposed on the entities in question were regrouped in a special book of the new Law. The book intentionally begins with a list of the obligations relating to the organisation and internal controls which those entities must establish. The legislation thus clearly indicates that these are essential conditions which these entities must first meet if they are to satisfy the legal obligations concerning vigilance over business relationships and transactions. These vigilance obligations, which include the identification and verification of the identity of the persons involved, knowledge of the customer, and of the purpose and nature of the business relationship or transaction, and constant vigilance in that regard, are now entirely governed by the principles of the risk-based approach. That approach permits less stringent preventive measures if the ML/TF risks are low, but stipulates tougher measures if those risks are high. The general adoption of this approach is intended to permit the optimum allocation of the prevention resources. In addition, the characteristics of this approach are now spelt out more clearly than before. In particular, the Law specifies that this approach must lead to a global risk assessment the results of which must be reflected in the internal policies and procedures of the entity concerned, combined with an individual assessment of the risks associated with each customer and intended to ensure that the vigilance measures applied are in keeping with the level and nature of those risks.

Similarly, the Law requires the supervisory authorities, including the Bank, to modulate the frequency and intensity of their supervisory functions according to the risk profile of each entity subject to supervision. That profile has to be ascertained by an assessment of the inherent risks confronting each entity on account of its own characteristics, combined with a risk management assessment taking account of the measures aimed at risk reduction and the degree to which those measures conform to the legal and regulatory obligations.

1.2 Bank Regulation of 21 November 2017

On 21 November 2017, to supplement this new legislative framework as required by the new Law, the Bank adopted a new Regulation [1] specifying the requirements to be met by the internal organisational arrangements of financial institutions under its jurisdiction, their general risk assessment process and their internal control measures and procedures. Unlike the Regulation that it replaces, this new Regulation no longer contains provisions on the duty of vigilance, as the obligations on that subject are now set out in full by the Law.

1.3 Implementation of the new legal and regulatory framework

As stated above, the overall risk assessment which the entities concerned must carry out and the adaptation of their internal prevention systems according to the risks identified are crucial elements of the new legal and regulatory framework. The Bank therefore decided to carry out checks without delay on all financial institutions under its jurisdiction. Accordingly, it requested all financial institutions to submit summaries of the results of their overall risk analyses, the weaknesses detected in their preventive systems, and the measures taken to remedy those weaknesses within a reasonable timescale [2].

1.4 Operationalisation of risk-based supervision

At the same time, without waiting for publication of the new Law, the Bank refined the tools at its disposal to base its checks on its risk assessment. Thus, to supplement the annual questionnaire concerning measures to combat ML/TF, hitherto focusing mainly on the level of conformity with the Laws and Regulations, the Bank requested financial institutions to supply relevant information on the inherent ML/TF risks that they face, taking account of sectoral differences [3]. The Bank also developed a tool enabling it to ascertain the risk profile of each of these financial institutions on the basis of all the available information. In accordance with the new Law, this approach has already enabled the Bank to determine its supervision priorities from 2017 onwards. On the basis of its experience, it thus produced a new periodic questionnaire including both questions on the inherent risks and on conformity with the new legal and regulatory framework, and questions designed to assess the effectiveness of the preventive measures applied by each supervised financial institution [4]. This new questionnaire, together with diversification of the

(1) National Bank of Belgium Regulation of 21 November 2017 on the prevention of money-laundering and terrorist financing, approved by the Royal Decree of 10 December 2017.

(2) Circular NBB_2018_02 of 24 January 2018 on the overall risk assessment of money-laundering and terrorist financing risks.

(3) Circular NBB_2017_15 of 24 April 2017 – Reporting on inherent risks related to money-laundering and terrorist financing to which financial institutions are exposed.

(4) Circular NBB_2018_01 of 15 January 2018 – Periodic questionnaire on combating money-laundering and terrorist financing.

information sources and additional improvements to the analysis tools, will enable the Bank to further enhance the quality of its risk-based approach.

2. Quality assurance

The Quality Assurance Unit set up in 2016 aims to give the Bank the assurance that its prudential supervision and resolution activities (in both the national and the international context) meet the quality requirements in terms of homogeneity and consistency, timeliness, accuracy, and conformity with the regulatory framework and best practices, which promote effective, efficient and rigorous supervision.

The strategic priorities, the intervention scope and the tools available to the Quality Assurance Unit, which reflect in operational terms the aims described above, and which were described in the Report 2016[1], continue to apply. The Quality Assurance Unit is currently continuing to work on the definition of its framework in order to progress towards a definitive operating method. In that connection, the intention is to define, in consultation with the various services concerned, a QA universe which will clearly specify the processes and activities of the various services operating in prudential supervision and resolution, but also to finalise in the near future a QA framework, which will structure the activities directly carried out by the Quality Assurance Unit and will also aim to provide methodological support for all the players concerned, whether their work is aimed primarily at improving the quality of their operation, or whether they act in the context of their day-to-day supervision activities.

The quality assurance work in the field of bank supervision, conducted as a priority in response to the ECB's expectations on the subject in the context of the SSM, continued in 2017 and focused in particular on the processes, procedures and checks applied in the operational services responsible for the supervision of less significant institutions (LSIs). A key development area which will become still more important in 2018 concerns managing and coordinating a network of quality assurance correspondents from the Bank's operational supervision and resolution services. A new platform was thus established for the regular, structured exchange of information concerning quality, but also for the purpose of determining, in consultation with the services concerned, any measures needed to improve quality in order to ensure that these services can work as effectively and efficiently as possible to achieve the four objectives stated above.

(1) See section F.2. under "Prudential regulation and supervision" in the Report 2016.

(2) The central point of contact for FinTech has its own web page on the Bank's website: https://www.nbb.be/en/financial-oversight/general/contact-point-fintech.

3. FinTech

3.1 Fintech contact point

Given the market's increased interest in innovation in financial technology, in 2017, the Bank established a single point of contact for FinTech on its website[2], in collaboration with the FSMA. The establishment of this contact point is in line with the strategy of the Minister of Finance and the HLEG on the future of the Belgian financial sector, which aims to promote Brussels as a financial centre. The contact point operates as an access channel to the supervisory authority for questions on the legislation governing the provision of financial services in Belgium. The target group comprises institutions that have exploratory questions on the provision of new and innovative financial products or services and which may require an authorisation by the regulator. The purpose of the contact point is therefore to function as a single, convenient point of contact for dealing with the various questions raised; the questions are either answered directly or forwarded to the appropriate contact persons. In that regard, the contact point acts as a facilitating entity and should not be considered a mandatory route for questions on FinTech.

Since the contact point was set up on 25 April 2017, there have been meetings on a regular basis with external parties who had questions on the legislative framework. Some of the enquiring parties were considering setting up a business, whereas other parties, including existing firms, were examining whether they should offer new financial services. The contact point staff found that the majority of the questions asked concerned the provision of payment services and, to a lesser extent, the creation of on-line exchange platforms for virtual and digital currencies. The main factor driving this trend is the second European Payment Services Directive (PSD2), which came into force at the beginning of 2018. Among other things, the Directive introduces new payment services and opens access to payment accounts for institutions approved for that purpose (see section F.2.). Most parties also had questions on the legal qualification of the services that they are considering offering, and the legal requirements related to the provision of those services in Belgium.

The contact moments with FinTech firms revealed that start-ups need to invest heavily and need to have substantial capital available to attain the necessary size on

their market. One of the key reasons for this is that a sufficient volume of users needs to be attracted for the firm to become profitable from the provided services.

In consultation with the organisations representing start-ups in the financial sector, an analysis was also conducted to identify the main obstacles that those firms encounter in expanding their activities. This analysis showed that the requirements concerning appropriate internal control systems were seen as a stumbling block by firms that have a limited number of full-time equivalents employed. Furthermore, although the necessary injections of capital are deemed to be significant, the sector does not perceive them as a constraint. Next, the analysis highlighted that a large part of the sector was unfamiliar with the various regulatory frameworks applicable to the financial sector. The single point of contact therefore often needs to provide regulatory guidance, thereby clearly explaining the authorisation procedure and qualifying the envisaged services. The Bank will continue to work on improving the visibility of the contact point in order to foster a dialogue between the supervisory authority and the sector. For that reason, in view of the potential influence of the new technologies on the Belgian financial market, a questionnaire was sent out during the year under review to the various players on the market, including the banking and insurance sector and payment institutions, to obtain additional information on the impact of FinTech and the digital transformation. This horizontal survey was aimed to gain a better understanding of the attitudes of the various players towards FinTech, the potential impact of these developments on their business model, and the measures they envisage for keeping up with developments.

3.2 Digital currencies

Digital currencies issued by the private sector (such as bitcoin) are different from regulated electronic money[1] in that they are not issued against a deposit of funds, and they have no fixed value in relation to a currency which is legal tender, such as the euro. Their issuers are not subject to the surveillance of the supervisory authorities and do not need authorisation to pursue their activities. Transactions in private digital currencies, both purchases of such currencies on exchange platforms and the transactions in which they are used as a means of payment, therefore take place outside the regulated financial system. They are called "currencies" because in some cases they can be used as a means of payment, but they do not have all the economic and legal characteristics of money. They are not genuine units of account, as it is only in very exceptional cases that prices are expressed directly in a private digital currency, and they cannot be regarded as a store of value, particularly on account of their price fluctuations. Moreover, they are not legal tender, nor do they have any discharging power. Creditors are therefore not required to accept them in settlement of debts (see box 1 under "Economic and financial developments" in this Report).

The escalating price of the bitcoin in 2017 once again attracted the attention of the media and the public to this phenomenon. The Bank, which had already stressed the risks that holders of these currencies incur in a warning published in 2014 and reiterated in 2015, continues to keep a close watch on developments in this sphere. The use of these currencies as a means of payment still appears marginal in Belgium. However, their use for criminal purposes or for terrorist financing has prompted the Belgian and European authorities to consider imposing rules on intermediaries who facilitate the conversion of private digital currencies into official currencies, the aim being to combat money-laundering and terrorist financing.

4. Cyber risks

4.1 Continuing rise in cyber threats

During the year under review, the already strongly computerised financial sector continued to digitalise its business processes. The degree of interconnection between the operational processes of the various financial players also remained very high. Furthermore, financial institutions increasingly opt for business models in which IT services are outsourced, according to operational or functional specialisation. Customers' access channels to financial institutions and FMIs are becoming increasingly digitalised and more diverse, yet another factor rendering the financial landscape more complex and leading to a higher operational risk level.

Cyber attacks directed at financial sector targets are becoming increasingly sophisticated and causing ever more damage (see box 17). The number of attacks compromising the integrity or confidentiality of IT systems and data is also on the rise. Cyber attacks may originate within or outside the institution, and the attackers may have various motives, such as financial theft, geostrategic espionage, and sabotage inspired by terrorist or militant ideas. This diversity makes it very difficult for financial institutions and FMIs to ensure that their IT systems, data and services are

(1) As defined in European Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

adequately protected against all types of attacks. Since cyber threats are evolving very rapidly, defensive capabilities of institutions and FMIs must be more flexible than ever in responding to changing patterns of attacks. It is vital to have solutions for collecting information on potential threats, attackers, and types of attack. One example of such a solution is the electronic portal installed by Febelfin in 2016 to facilitate the exchange of information on cyber security between all parties concerned.

It is also useful for financial institutions to know the risk profile of the customer and/or counterparty when it comes to determining the fraud risk for specific transactions. In retail banking, this is being achieved for example by integrating security mechanisms in the internet or mobile banking applications. In the context of correspondent banking activities, the Customer Security Programme (CSP) currently being implemented by SWIFT is an important example of a development aimed at facilitating risk assessment.

Box 17 – Some examples of cyber security incidents in 2017

Lloyds Banking Group: in January, a number of major banks in the United Kingdom experienced a wave of Distributed Denial of Service (DDoS) attacks lasting for three days. These attacks caused partial non-availability of digital channels, but did not result in any fraud or data leaks.

Operation Cloud Hopper: in April, PwC conducted a study on Operation Cloud Hopper which shows how providers of IT services (such as cloud services) were hacked in order to spy on their customers and steal confidential documents. There are no direct indications that financial institutions were targeted, but the *modus operandi*, namely attacking indirectly via the IT service supply chain, is worrying.

Wannacry/Petya/NotPetya/Nyetya/Goldeneye: from May, a series of large-scale ransomware incidents have been observed. Ransomware is malware which digitally encrypts a user's data until the victim pays a ransom (generally in bitcoin). The various versions of ransomware are probably based on a source code previously stolen from the US National Security Agency. Belgian financial institutions proved adequately protected against this wave of attacks, but a number of foreign institutions suffered serious difficulties.

Equifax: in July, the personal data of 143 million American residents were stolen from Equifax, a credit-rating company. The data leak caused a significant fall in the company's stock market value.

Silence Trojan: in November, Kaspersky Lab discovered the malware Silence Trojan, which targets financial institutions and is similar to Carbanak. According to Kaspersky, in 2015, up to 100 financial institutions (particularly in Eastern Europe and Russia) were infected with the Carbanak malware which, they claim, may have resulted in fraud amounting to $ 1 billion. In this type of attack, fraudsters attempt to penetrate financial institutions directly, to then accumulate knowledge of the victim's internal systems over prolonged periods (several months) before proceeding to act and stealing substantial sums. At this stage, it is not known whether Silence Trojan has already claimed any victims.

During the year under review, as in previous years, cyber risks formed the subject of ever closer attention in the financial sector. Assessing cyber risks and promoting control of those risks are also top priorities for the prudential supervision and oversight of financial institutions and FMIs. At individual level, institutions are being strongly encouraged to continue stepping up their measures and efforts to protect against cyber risks. Cross-sectoral cyber risk management strategies under development in Belgium and abroad also remain a focus of attention.

4.2 Recommendations on cyber resilience

On 1 January 2016, the Circular[1] on the Bank's expectations concerning the operational continuity and security of systemically important institutions came into force. Cyber resilience is a major theme addressed in

(1) Circular NBB_2015_32 of 18 December 2015 on additional prudential expectations concerning the operational continuity and security of systemic financial institutions.

this Circular. The Bank also made an active contribution to establishing a European regulatory framework for the management of IT risks and cyber risks under the aegis of the EBA. That work culminated in the EBA's publication of guidance for supervisory authorities on the assessment of the ICT risk in the SREP of credit institutions and investment firms[1] and recommendations on outsourcing by financial institutions to cloud service providers[2]. Finally, the EBA published technical standards, guidance and recommendations in the context of the second European Payment Services Directive (PSD2), where cyber-security-related risks are being addressed.

In June 2016, the CPMI and IOSCO had published guidance[3] on cyber resilience for FMIs that entered into force immediately. In September 2017, the CPMI published a discussion note[4] presenting a strategy aimed at reducing the fraud risk in wholesale payments, and developing measures to prevent, detect and remedy fraud, by providing for proper communication on the subject by all public and private sector players concerned. As co-chair of this CMI working group, the Bank made a significant contribution to that note. In the near future, the CPMI will draw up recommendations spelling out the proposed strategy.

One of the main attention points in prudential regulation and oversight recommendations is the need for the management of cyber risks by the financial players. Controlling cyber risks not only depends on implementing technology solutions, but also entails sufficient attention to address threats that originate from within the organisation, either by employees or management. Financial players must make their staff aware of cyber risks so that they know how the risk can arise and how they should respond. Likewise, the management bodies must have the necessary expertise and information to be able to monitor cyber threats effectively and keep them within acceptable limits.

The publications mentioned above likewise recommend that financial players conduct tests to assess their degree of resilience against cyber threats. Those tests are becoming increasingly sophisticated and in some jurisdictions they are based on specific frameworks comprising a harmonised test methodology. The Bank is actively monitoring developments in this area to ensure that sound management practices in this regard are also being established in Belgium, taking into account any relevant European or international initiatives on the subject.

(1) EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP).
(2) EBA Recommendations on outsourcing to cloud service providers.
(3) CPMI-IOSCO guidance on cyber resilience for financial market infrastructures.
(4) BIS, Discussion note – Reducing the risk of wholesale payments fraud related to endpoint security – consultative document, September 2017.

4.3 Operational activities

The Bank devotes specific attention to cyber risks as part of its prudential supervision and oversight work, on the one hand focusing on the security posture of individual financial institutions and FMIs and the confidence that they inspire, and, on the other hand, on the situation of the sector as a whole.

The approach to address cyber risk management at individual institutions is two-pronged. First, institutions are required to hold capital to cover their exposure to operational risks, including cyber risks. Second, the operational security and robustness of the critical processes of financial institutions and FMIs are subject to close monitoring. The availability, integrity and confidentiality of the IT systems and data play a central role here. In 2017, the Bank conducted a number of inspections to check the supervised entities' compliance with the regulatory framework and the proper management of their IT systems in relation to cyber risks. In addition, the Bank also monitors cyber risks at financial institutions and FMIs on an ongoing basis as part of its continuous and recurrent supervisory activities.

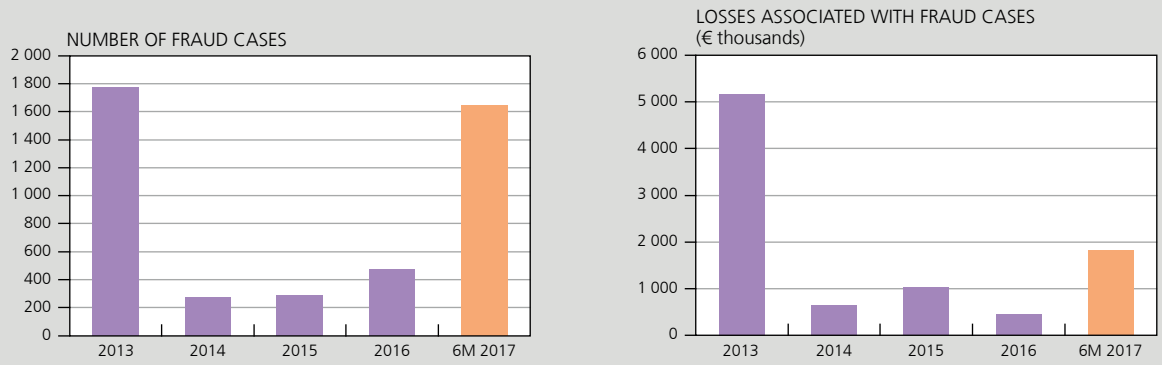
The Bank also devotes the necessary attention to sector-wide initiatives concerning cyber risks. An important example in this regard is its contribution to the development of a framework for ethical hacking (red teaming), an initiative linked to the objectives of both the Belgian Financial Sector Cyber Advisory Council and the ECB's FMI Cyber Security Strategy. In the SSM, a framework for reporting cyber risk incidents was set up in 2016, and sector-wide surveys and analyses on cyber themes are being conducted on a regular basis.

4.4 E-banking fraud

In 2017, the Bank continued its close cooperation with Febelfin and other parties to jointly follow up on e-banking fraud and to continue raising consumers' awareness on the subject. Despite these efforts, it was noted that the number of e-banking fraud cases and the associated financial losses increased considerably in the first half of 2017.

As in previous years, reported cases of e-banking fraud among consumers in 2017 were due almost exclusively to fraud techniques whereby cyber criminals deceive users of e-banking into disclosing their personal security codes (usually after a telephone call or via a malicious website). The rise in fraud cases in 2017 is therefore attributable to an increase in the number of attacks rather than the use

CHART 93 E-BANKING FRAUD



Source: Febelfin.

of innovative fraud techniques. Here, too, the Bank keeps a very close watch on recent developments concerning authentication techniques for payments.

5. Developments in governance, reporting and auditors' cooperation in prudential supervision

The year under review saw the Bank adopt and publish a number of new normative documents on governance, reporting and auditors' cooperation in prudential supervision. In a first Circular, supervised undertakings are asked to implement a number of recommendations concerning their internal organisation to ensure that the supervisory authorities are sent prudential and financial data that meet high-quality criteria. The second Circular defines the auditors' duty to cooperate in prudential supervision. There are some major changes here in regard to the auditor's obligations concerning periodic reporting to the supervisory authority, both for the planning of its supervisory tasks and for their execution. A third Circular concerns the updating of credit institutions' and insurers' reporting obligations to the supervisory authority on loans to senior management, shareholders and/or related persons. Finally, the Bank also adopted a new version of the Circular and the Communication on the prudential assessment of acquisitions and increases in qualifying holdings in financial sector entities, in accordance with the common guidelines drawn up by the EBA, EIOPA and the European Securities and Markets Authority (ESMA). Mention should also be made of the legislative work aimed at strengthening the "fit and proper" framework and in relation to the conditions on performance of the compliance function.

5.1 Data quality Circular

In connection with their prudential supervision work, the supervisory authorities (the Bank, the ECB and – depending on the case – the EBA or EIOPA) periodically collect prudential and financial data from all institutions subject to their supervision. This reporting takes place at both national and European level.

For prudential supervision, good-quality reporting is essential: it ensures that the supervisory authority can conduct a solid, comparable analysis of the reported data and maintain a soundly-based dialogue with the institutions.

As the institutions are responsible for the quality of the data reported for prudential supervision purposes, the Bank deemed it useful to issue a set of recommendations to the institutions under its supervision, stating its expectations as regards prudential reporting quality.

For that purpose, a Circular[1] was adopted, setting out the criteria for assessing reporting quality. Those expectations concern not only the submission of the reports but also their content. They also include the various quality rules on reporting, drawn up by the supervisory authorities.

In addition, this Circular specified the prudential expectations regarding the internal organisation of institutions for the preparation and submission of prudential reports. Implementation of the principles of this Circular will at least ensure conformity with the quality requirements defined in

(1) Circular NBB_2017_27 of 12 October 2017 on the Bank's expectations as regards quality of reported prudential and financial data.

the regulatory framework on reporting. Accredited auditors are asked to examine compliance with these prudential expectations in the six-monthly reporting checks.

5.2 Duty of cooperation of accredited auditors

In view of the societal importance of financial institutions and insurance companies, auditing duties can only be entrusted to auditors approved for that purpose by the Bank. In addition, the sectoral laws stipulate that accredited auditors must, on their own exclusive responsibility, cooperate in prudential supervision. That obligation implies that they perform certain specific tasks, which are spelt out in a new Bank Circular[1].

That Circular replaces an earlier Bank Circular dating from 2012, although the latter's structure has been largely retained. First, the Circular takes account of the new legislation which has entered into force since the publication of the previous Circular and which applies to credit institutions, investment firms and insurers/reinsurers respectively. The Circular now also includes the details of the duty of cooperation in the case of accredited auditors of electronic money institutions.

In addition to the necessary regulatory updates, a number of changes were made in order to augment the value added of the accredited auditor's role in the confirmation of periodic financial reporting. Thus, in the course of their activities, auditors are asked to focus particularly on a number of sector-specific prudential points for attention. The importance of the accredited auditor's role in ensuring the quality of the figures is also emphasised (see also section G.5.1). Furthermore, accredited auditors of general interest entities (credit institutions, insurers and reinsurers, settlement institutions and entities equivalent to settlement institutions) are required to submit their audit plans systematically to the supervisory authority and to produce supplementary reports, notably on important subjects which attracted their attention in the course of their work.

The new Circular also takes account of the changes resulting from the entry into force of Solvency II. The accredited auditor's duties regarding periodic statements are complicated by the fact that the Solvency II legal framework is no longer based on the accounting framework (BE GAAP/IFRS), the traditional point of reference for this work. Only the parts of the Solvency II reporting that permit a better understanding of the institution's financial situation are included in the external audit, unlike the parts prepared primarily for statistical purposes. From now on, accredited auditors must take account of the reporting introduced under Solvency II for the work of assessing internal control measures.

Finally, the Circular conforms to the guidelines published by both the EBA[2] and EIPOA[3] on communication and dialogue between the supervisory authority and statutory auditors.

5.3 Loans, credit and guarantees to managers, shareholders and related persons

Article 72 of the Banking Law and Article 93 of the Solvency II Law define the legal framework for loans, credit and guarantees granted to managers, shareholders and related persons. These legal provisions prescribe reporting to the supervisory authority.

The adoption of the Banking Law in 2014 and the Solvency II Law in 2016 fundamentally changed the legal regime. In view of these and subsequent changes, it was necessary to replace the old 1994 Circular[4] on the subject.

The new Circular[5], aimed at both the banking sector and the insurance sector, sets out the legal provisions and clarifies the way in which institutions must fulfil their annual reporting obligations to the supervisory authority. In the annex to the Circular, tables provide the supervisory authority with a complete picture of the total outstanding amount in relation to a particular person or institution.

Credit institutions must submit their report to the supervisory authority before the end of February in the following year. Insurance undertakings must submit these tables in conjunction with the updated governance memorandum, with due regard for the deadlines stated in the eCorporate 2016/40 Circular.

5.4 Supervision of qualifying shareholders

On 5 May 2017, the EBA, EIOPA and ESMA published new joint guidelines on the prudential assessment of acquisitions and increases of qualifying holdings in the financial sector entities.

(1) Circular NBB_2017_20 of 9 June 2017 on the duty of cooperation of accredited statutory auditors.
(2) EBA Guidelines of 7 November 2016 on communication between competent authorities supervising credit institutions and the statutory auditor(s) and the audit firm(s) carrying out the statutory audit of credit institutions.
(3) EIOPA Guidelines of 2 February 2017 on facilitating an effective dialogue between competent authorities supervising insurance undertakings and statutory auditor(s) and the audit firm(s) carrying out the statutory audit of those undertakings.
(4) Circular D1 94/5 of 28 November 1994 on loans, credit and guarantees to managers, shareholders and related persons.
(5) Circular NBB_2017_21 of 7 July 2017 on loans, credit and guarantees to managers, shareholders and related persons.

Following that publication, the Bank revised its regulatory framework on shareholder supervision for (a) credit institutions under Belgian law, (b) insurance and reinsurance undertakings under Belgian law, (c) investment firms under Belgian law, (d) financial holding companies under Belgian law, (e) insurance holding companies under Belgian law, and (f) mixed financial holding companies under Belgian law.

The Communication[1] published by the Bank in September 2017 replaces the 2009 Communication[2] and forms the new reference framework for acquisitions, increases, reductions or transfers of qualifying holdings in the capital of one of the aforesaid financial entities. It provides all persons concerned with the necessary information for submitting their plans to the supervisory authority (the Bank or the ECB, depending on the case), and clarifications concerning the rules of procedure and assessment criteria that the supervisory authority will apply.

The main changes compared to the 2009 version concern (a) extension of the scope of the Circular, (b) redefinition of the concept of an indirect shareholding, (c) updating of the information required to assess the integrity of candidate shareholders who are natural persons and the effective management of shareholders who are legal persons, and (d) reinforcement of the requirements concerning continuous shareholder monitoring.

To supplement this Communication, the Bank published on the same day a new Circular[3] for the attention of financial entities in which it specifies the arrangements for implementing the occasional and periodic notification obligations that these financial entities are required to fulfil concerning their shareholders. That Circular replaces the 2009 Circular[4] on the same subject.

5.5 HLEG recommendations on fit and proper and compliance

The 2016 report of the High-Level Expert Group (HLEG) on the future of the Belgian financial sector (see also chapter B above) contains a set of recommendations on strengthening governance in financial institutions. Subsequently, proposals were drawn up in consultation with the various stakeholders concerning the fit and proper assessment of senior management and the compliance function in financial institutions. That process resulted in changes to various sectoral laws.

In regard to "fit and proper", members of the statutory governing body, persons who effectively run the undertaking, and those responsible for independent control functions must at all times have the necessary professional integrity and sufficient expertise to perform their function. The legislative changes aim to reinforce the permanence of those requirements.

On the one hand, they introduce the obligation to inform the supervisory authority immediately of anything implying a change in the information supplied at the time of the appointment which could affect compliance with the fit and proper requirements. This list is not exhaustive, but it may include new, relevant facts or information such as investigations initiated by the administrative or judicial authorities in the broad sense (including investigations into facts which could give rise to disqualification), information which could lead to disciplinary sanctions, etc.

They also enable the supervisory authority to decide to reassess the fit and proper character of those concerned on the basis of findings or analyses conducted during the exercise of its supervisory mission, or if it has new information relevant for the assessment of them. That reassessment may, for example, result in reports or findings demonstrating a negative or hostile attitude towards generally accepted good practices (e.g. regarding the transparent and complete disclosure of information to the statutory governing body), recurrent or deliberate disregard of supervisory authority recommendations, a proven non-availability for attending meetings, the supply of incomplete or incorrect information to the supervisory authority or shareholders, an uncooperative attitude towards the supervisory authority, etc. This incorporation of the fit and proper policy into the continuous supervision of institutions is in line with the international and European trend towards making the top management more responsible for its actions or omissions. For instance, in its guide to fit and proper assessments, the ECB stresses the importance of new facts relating to performance of the function which may generate doubts about the staff member's ability to ensure the sound and prudent management of the institution.

The legislative changes concerning compliance aim to provide a stronger framework for this function in order

(1) Communication NBB_2017_22 to candidate shareholders and assigning shareholders.
(2) Communication CBFA_2009-31 of 18 November 2009 to persons intending to acquire, increase, reduce or sell a qualifying shareholding in the capital of financial institutions.
(3) Circular NBB_2017_23 of 22 September 2017/Circular to financial institutions concerning acquisitions, increases, reductions and transfers of qualifying holdings.
(4) Circular CBFA_2009_32 of 18 November 2009 to financial institutions concerning acquisitions, increases, reductions and transfers of qualifying holdings.

to promote the integrity of institutions and confidence in the financial sector in general. More specifically, they concern :

- specifying the responsibility of the statutory governing body in drafting the integrity policy ;
- stipulating that the statutory governing body must submit an annual report to the supervisory authority on the assessment of the proper functioning of the compliance function ;
- in cooperation with the FSMA, enabling the Bank to make those in charge of the compliance function subject to the same minimum criteria concerning expertise as those already implemented by the FSMA.

On this last point, the Bank and the FSMA have developed a joint approach to encourage harmonisation of the requirements of the two supervisory authorities for the assessment of the expertise of those in charge of the compliance function. The Bank set out that approach in a draft Regulation. The FSMA also drew up a Regulation amending its previous Regulation of 27 October 2011 on the approval of compliance officers.

The Bank's draft Regulation begins by listing the requirements for the assessment of the expertise of the person responsible for the compliance function, the main new requirement being that the person must pass an examination at a training centre approved by the Bank and the FSMA. Next, it describes the rules on approval of the examination, which will form the subject of a protocol of collaboration between the two supervisory authorities to ensure the effective and consistent implementation of the Regulation. Finally, it contains a number of essential transitional measures.