E. Digitalisation

Financial services digitalised further in 2022. This trend has allowed consumers, employees and businesses to cope with various challenges, including the COVID-19 pandemic, in recent years. Examples of developments in digitalisation include new business models based on innovative payment solutions, the use of machine/deep learning or the automation of processes by robotics to increase operational efficiency, the refinement of business strategies through artificial intelligence and data analysis, and the use of cloud services for IT infrastructure management and data aggregation. The idea is often to anticipate expected fundamental changes in the structure of the financial services market. The role of financial services and actors is indeed changing significantly on a global scale. Both financial and non-financial services are increasingly using integrated payment, e-commerce and social media platforms and collaborative ecosystems. Innovation is facilitated in particular by the use of modular technologies that allow different financial and non-financial actors to communicate via application programming interfaces (API).

All of these developments have already had a major impact on the risks to financial institutions, consumers, monetary policy and/or financial stability. As digitalisation leads to increased interconnectivity, it is in particular becoming increasingly crucial to ensure the (cyber)security and continuity of underlying systems. There is every reason to believe that the risks inherent in digitalisation will only increase in the foreseeable future.

Against this backdrop, the European Commission has proposed a strategy to foster digital innovation, the creation of a digital single market for financial services and a European financial data space to facilitate access to and the sharing of financial data. The strategy also aims to achieve greater control of the risks brought about by digital innovation. It has led to a series of European legislative initiatives, with which the Bank is closely associated.

Two of these, relating to operational resilience and crypto-assets, are described below. Another regulatory initiative, to define harmonised rules for artificial intelligence, launched in April 2021 by the European Commission, is also examined, along with the Bank's actions in support of the ECB's digital euro project and efforts to map fintech/insurtech developments in supervised institutions and mitigate the cyber and IT risks to which they are exposed.

1. The digital euro

Since the Bank's last annual report, extensive discussions have been held with all parties involved in the design of a digital euro. The main objectives of a digital euro would be to further boost digitalisation and the efficiency of the European economy while enabling strategic autonomy, without creating additional competition for private payment solutions. In October 2021, the Eurosystem launched a 24-month study phase on the digital euro project in order to finalise decision-making on the main design and distribution issues and to develop a prototype.

One of the key decisions taken so far pertains to the transfer mechanism. In particular, it was decided that the Eurosystem will further explore a third-party validated online solution as well as a peer-to-peer offline solution. In the former, transactions take place online and are validated by a trusted authority, while the latter involves transactions conducted between two users through a suitable device (e.g. a smartphone), without an online mode. The time to market for the latter solution is more uncertain due to its dependence

on near-field communication (NFC) technology. It is important that the development of a third-party validated online solution not be delayed should the timely delivery of a peer-to-peer offline solution prove unfeasible.

In recent months, extensive consideration has also been given to what the public considers the most important feature of the digital euro, namely privacy. Initially, it was thought that the current anti-money laundering and privacy protection practices of private-sector digital solutions would be maintained as a baseline scenario. However, it has since been decided that the Eurosystem will explore two additional options that differ from the above solutions, in the interest of privacy protection. These options are selective privacy for low-value online payments and offline functionality that keeps users' balances and transaction data private. Further research is needed to determine how these two options can be implemented, either within the current regulatory framework or through new bespoke regulations. In addition, various technologies are being tested to improve the privacy of the online solution. In any case and in accordance with what has been decided by the ECB Governing Council, the Eurosystem is committed to ensuring the highest possible level of privacy in the regulatory framework.

Finally, the Eurosystem recently took an important step to safeguard financial stability, by exploring tools to control the amount of digital euro in circulation in order to prevent the use thereof for investment purposes. Discussions have been held on both quantitative limits on digital euro holdings by individual users and remuneration-based tools that could be calibrated to discourage digital euro holdings above a certain threshold. Both options will be considered in the design of the digital euro, so that the appropriate tools and parameters can be defined closer to the time of issuance and remain flexible in the future.

At the time of writing, the Eurosystem was still actively engaging with all stakeholders and will continue to do so for the rest of the investigation phase, with a further round of focus groups planned for completion of the prototype. The Eurosystem will decide in autumn 2023 whether to issue a digital euro. If the project receives the green light, it will move towards the realisation phase. This phase is expected to last around three years and will focus on the development and testing of technical solutions and the business arrangements necessary for a digital euro.

2. Fintech

2.1 Prudential treatment of crypto-asset exposures and the draft EU regulation

Draft EU Regulation on Markets in Crypto-Assets (MiCA)

Recent events in the stablecoin markets, such as the TerraUSD debacle and the collapse of the cryptocurrency exchange FTX, have highlighted the importance of consumer protection when it comes to crypto-assets. Some stablecoins, which are linked to the value of official currencies such as the euro, also pose a risk to payment systems or monetary sovereignty if accepted as a means of payment. This justifies a legislative initiative.

The proposal for a Regulation on Markets in Crypto-Assets (MiCA) aims to address these crypto-asset risks. A political agreement was reached on this proposal in June 2022, following interinstitutional negotiations (trilogues) between the European Parliament, the Council and the Commission.

MiCA targets crypto-assets not covered by existing regulations, particularly on financial instruments and electronic money.

This regulation applies to various actors: issuers that offer crypto-assets to the public[1] or that seek admission to trading on a crypto-assets market as well as crypto-asset service providers.

MiCA provides for three distinct frameworks depending on the category of crypto-asset (see table E.1). The first two asset categories consist of stablecoins, which are linked to the value of a currency or other assets. Stablecoins are further divided into e-money tokens and asset-referenced tokens, depending on their reference asset. The third category is a residual category that covers all other crypto-assets. By including this category, the legislature wishes to regulate all crypto-assets.

1 An offer to the public consists of the disclosure of information enabling potential holders to purchase crypto-assets, for example via a website.

Tableau E.1

Crypto-asset categories under MiCA

	Stablecoins		Other crypto-assets
	E-Money Token	Asset-referenced Token	
Reference asset	An official currency	A basket of official currencies or other assets e.g. gold	Do not aim to maintain a stable value relative to a reference asset (e.g. utility tokens)[1]

Source : NBB.
1 The main function of a utility token is to provide future access to a company's goods or services.

The first set of rules applies to parties that offer crypto-assets to the public or that request admission to trading on a crypto-assets market. These are primarily issuers of crypto-assets.

Firstly, issuers are required to apply for a prior authorisation. In the case of e-money tokens, only credit and electronic money institutions will be authorised as issuers. MiCA also contains consumer protection requirements, such as a right of redemption at any time at the market value of the reference asset. To ensure redemption, issuers must establish and maintain a reserve of sufficiently liquid and secure assets. Issuers are also subject to conduct and transparency rules, as well as capital, liquidity, governance and risk management requirements. Finally, the white paper[1] for asset-referenced tokens requires prior approval, while that for e-money tokens requires only prior notification to the competent authorities.

Stricter rules, particularly in terms of capital requirements and liquidity management, apply to issuers of asset-referenced tokens and e-money tokens considered significant in view of the impact they could have on financial stability. For the offering to the public and admission to trading of the third category of crypto-assets (residual assets), the white paper requires only prior notification to the competent authorities. Persons offering such assets to the public are also subject to rules of conduct and other specific obligations.

1 The white paper is a document drafted and published by and under the responsibility of the issuer, containing the key information required to be published in accordance with MiCA (relating to the issuer, the project, the type of asset and the rights to the asset and the technology) in order to allow potential purchasers of the crypto-asset to make informed decisions.

The second set of rules relates to providers of crypto-asset services such as crypto-asset custody, operation of a trading platform and order execution. Such providers are subject to prior authorisation or prior notification in the case of certain institutions – such as credit institutions – that are already subject to a prudential framework. These rules apply in full to service providers of crypto-assets for which the issuer is difficult or impossible to identify, such as Bitcoin.

MiCA will be applicable 18 months after its entry into force, except for the provisions related to asset-referenced tokens and e-money tokens, which will apply 12 months after the entry into force.

Prudential treatment of crypto-asset exposures by the Basel Committee on Banking Supervision (BCBS)

Although banks currently have limited exposure to crypto-assets, the continued growth of and innovation on the markets for crypto-assets and services are generating increasing interest from the banking sector. This development could pose new risks to financial stability and the banking system.

Against this backdrop, the BCBS approved in December 2022 a standard on the prudential treatment of banks' exposures to crypto-assets. This standard, which was preceded by two public consultations in 2021 and 2022, classifies such exposures into two groups, based on certain characteristics of the crypto-assets involved (see chart E.1) :

- The first group includes assets deemed eligible for treatment under the existing Basel framework, subject to certain modifications and additional guidance. This group is further divided into two sub-groups: tokenised traditional assets[1] (Group 1a) and stablecoins[2] (Group 1b). To qualify for this group, assets must meet conditions regarding *inter alia* (1) the legal framework for the rights and obligations arising from the asset, (2) the transferability and settlement finality of transactions involving the asset, and (3) the identification, regulation, supervision or risk management framework of players that form part of the asset's ecosystem (those that provide redemptions, transfers, validation of transactions, investment of the asset reserve, etc.). For stablecoins, it is required that the issuer be regulated and supervised and subject to prudential capital and liquidity requirements and that the stabilisation mechanism be robust.

  In general, assets in the first group will be subject to capital requirements based on the weighted risks of the underlying exposures under the Basel framework. If the technological infrastructure of the asset in question presents specific weaknesses, an additional risk-weighted asset (RWA) requirement will be applied to cover the risks inherent in it.

- The second group consists of assets that do not meet all conditions to qualify for the first group. These assets are also divided into two subgroups and will in principle be subject to new conservative prudential treatment (Group 2b) consisting of the application of a risk weight of 1 250 % to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the crypto-asset. However, the standard proposes to recognise hedging for selected crypto-assets in the second group that meet certain criteria (Group 2a). Exposures to these assets (and related derivatives) will be subject to a modified version of the standard or simplified standard approach to market risk.

- Finally, exposures to assets in the second group are limited to 1 % of Tier 1 capital. If this limit is exceeded, the amount in excess of 1 % will be subject to the more conservative Group 2b capital requirements. Moreover, if the exposure exceeds 2 % of Tier 1 capital, the full exposure will be subject to the Group 2b requirements.

- Other requirements (related to operational risk, liquidity risk, leverage ratio, large exposures, etc.) apply to all categories of crypto-assets.

The proposed treatment is summarised below.

One of the most contentious issues in the consultation responses was the eligibility of stablecoins for the first group of crypto-assets. It was proposed that crypto-assets be required to pass two tests in order to qualify for this group.

- The first test aims to ensure that the asset can be redeemed at any time at the market value of the reference asset. This test includes a series of conditions related to the type of stabilisation mechanism and the guarantees it provides. In particular, the mechanism must be supported by a sufficiently large asset reserve. This test was retained in the standard ultimately adopted.

- A second test aimed to ensure that the holder could sell the asset on the market at a price close to the market value of the reference asset. This test set a tolerance limit for the deviation of the market value of the asset from the market value of the reference asset, measured over a 12-month period. The intention was to supplement the first test with an assessment of the likelihood of the asset being repurchased at the market value of the reference asset. This test was abandoned, but the possibility of developing statistical tests to identify low-risk stablecoins will be revisited by the end of 2023.

A second point for discussion was whether so-called "permissionless"[3] assets are eligible for Group 1. Such assets will be excluded from Group 1, but this status will be reassessed by the end of 2023.

The standard will apply as from 1 January 2025.

1 Tokenised traditional assets are digital representations of traditional financial assets acquired through cryptography, distributed ledger technology (DLT) or similar technology that records ownership of the assets.

2 Stablecoins are crypto-assets that aim to maintain a stable value relative to a specific asset or a pool or basket of assets.

3 In distributed ledger technology, the term "permissionless" refers to a particular configuration of this technology in which users and nodes (i.e. computers that host a copy of the ledger and participate in the recording of transactions) do not need to be authenticated or authorised.

Chart E.1

Structure of the prudential treatment of crypto-asset exposures (Basel Committee on Banking Supervision)[1]

Source: BCBS.
1 Prudential treatment of crypto-asset exposures (December 2022).

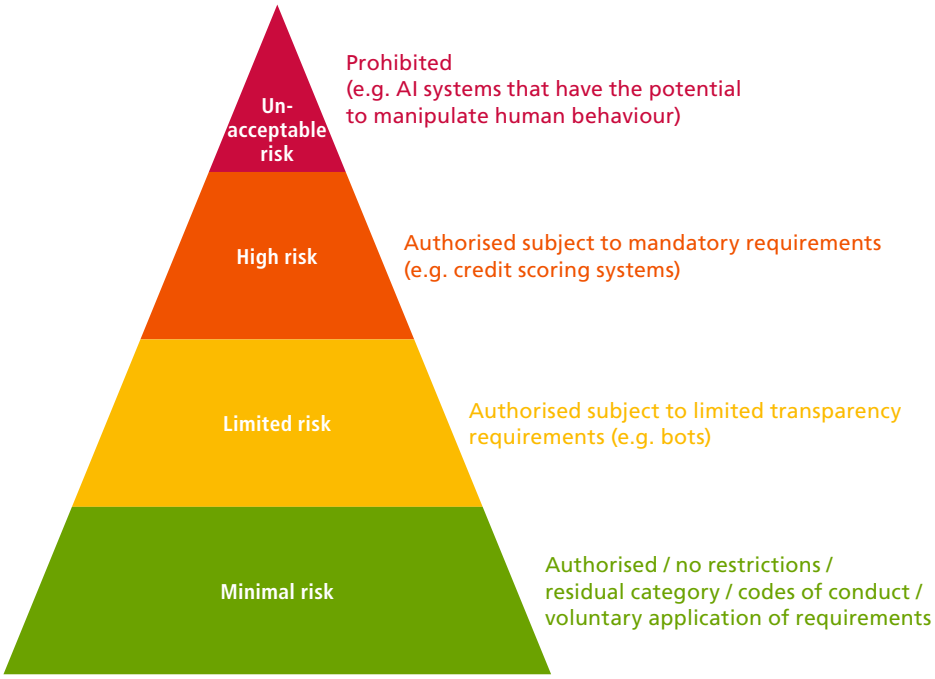
2.2 Regulation on artificial intelligence

Regulation on artificial intelligence (AI) and the impact thereof on institutions providing credit rating systems and certain life and health insurance systems

On 21 April 2021, the European Commission published a proposal for a regulation laying down harmonised rules on AI in order to safeguard fundamental rights while fostering innovation. This regulation concerns the development, marketing and use of AI systems in the Union and follows a proportionate, risk-based approach, ranging from a total ban to voluntary application of requirements (see chart E.2): (1) AI systems that pose an unacceptable risk (such as those that have the potential to manipulate human behaviour) are prohibited;

Chart E.2

Proposal for a regulation on artificial intelligence, risk-based approach[1]



Source: NBB.

1 See also https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

(2) so-called high-risk AI systems that pose a significant risk to fundamental rights are subject to strict requirements, which will be further specified in harmonised standards; (3) certain systems that pose more limited risk (emotion recognition systems, systems interacting with humans) are subject to limited transparency obligations aimed at informing human users that they are interacting with an AI system; (4) other systems deemed to pose minimal risk are not subject to mandatory requirements, but the creation of codes of conduct aimed at encouraging the voluntary application of the requirements applicable to high-risk AI systems is facilitated and encouraged.

In November 2022, the Council adopted a general approach and initiated inter-institutional negotiations (trilogues) between the European Parliament, the Council and the Commission. The risk-based approach was hereby confirmed. Potentially high-risk systems are listed in an annex. They include (1) AI systems used to evaluate the credit score or creditworthiness of natural persons and (2) AI systems used for risk assessment and pricing, for natural persons, in life and health insurance products. All AI systems listed in this annex are considered high-risk unless their output plays a purely accessory role in the human decision-making or action in which they are used.

Like the Commission's proposal, the general approach aims to introduce a preventive system that relies primarily on (1) the use of conformity assessment procedures by AI system providers and (2) the monitoring of these procedures. An AI system provider falls under the proposed rules if it develops an AI system or has an AI system developed and places it on the market or puts it into service under its own name or under a registered trademark.

Providers of high-risk AI systems will be subject to additional obligations, such as the introduction of a risk management system, appropriate governance practices, data management and human oversight to allow the user to decide not to use or to discontinue the system.

2.3 Fintech survey and analysis for credit institutions

In 2017, the Bank launched a survey on fintech and digitalisation covering selected banks and financial institutions. This survey provided a general picture of the impact of fintech on the Belgian financial sector and facilitated the launch of a dialogue with market players on various digital themes. The analysis of the survey responses was communicated to the participants and the public in 2018, together with a range of best practices concerning governance, organisation and monitoring in regard to fintech and digitalisation.

In view of technological and market developments, a new survey was conducted by the Bank in 2020, the results of which were communicated to banks in 2021 and released in a public report in 2022.[1] The report revealed that banks had generally made progress in their digital transition, but that the speed of this transition varied across the Belgian banking sector.

Around the same time as the Belgian survey, the European Central Bank took initiatives on digitalisation and fintech within the SSM. The supervisory and risk assessment priorities of the SSM for 2022-2024 include addressing structural weaknesses in business models via effective digitalisation strategies and enhanced governance. In this context, the ECB has been working together with the European national supervisory authorities (including the Bank) to improve its market intelligence. As a first step, it held an industry consultation on digital transformation and the use of fintech. In a second stage, it launched a broader survey on these topics amongst significant credit institutions in the summer of 2022, which allowed it to collect information that was not available in a consistent and coordinated way within the SSM. The results of this survey will be instrumental in (i) setting prudential priorities, (ii) identifying issues requiring further assessment, and (iii) developing guidance for SSM supervisors to assess risks and setting prudential expectations for banks. The main findings are also relevant for shaping the SREP methodology on business models and governance for the use of new technologies.

2.4 Insurtech survey and analysis of insurance undertakings

Technological innovation is increasingly impacting the business model of insurance undertakings. The rapid pace of change brought about by technological innovation creates opportunities for both start-ups and established technology companies to provide financial services and also allows traditional insurers to adapt and improve their business models, services and products. However, these new trends can also create or reinforce certain risks.

In order to gain a better understanding of this evolving landscape and the current state of play in this field, the Bank carried out a survey of insurance undertakings. The first objective of the survey was to get a picture of insurers' vision and strategy with regard to insurtech and digitalisation. Companies indicated that digitalisation had increased operational efficiency and customer satisfaction, but that the race for talent made it difficult to pursue innovation.

Companies were then asked to provide a detailed overview of the technologies they are using or developing. The responses showed that companies clearly rely on mainstream technologies, such as the cloud. They also make extensive use of more innovative technologies, such as artificial intelligence and ecosystems. It was also found that digitalisation is present in virtually all aspects of the value chain, but mainly in distribution or underwriting and claims management. The analysis further revealed that innovation was mainly concentrated in non-life lines of business, including motor vehicle and fire insurance.
Finally, when asked about the risks associated with innovative digitalisation, insurance undertakings reported increased cyber risk and operational risk. They indicated that, in some cases, profitability was also affected, but that they were taking the necessary steps to manage these risks.

1 bfw-digitaal-editie2-2022-03-artikel-begassededhaem-mention-romont.pdf (financialforum.be).

3. Digital operational resilience

3.1 Cyber and IT risks

In terms of cyber and IT risks, 2022 was still characterised to some extent by the effects of the COVID-19 pandemic. However, the challenges associated with this event, such as massive recourse to home working, more limited physical presence of operators, specific attack patterns, etc., have been adequately dealt with in the financial sector. The solutions adopted now form part of the "new normal".

The financial sector's exposure to these threats increased following Russia's invasion of Ukraine. In February 2022, the geopolitical conflict in Eastern Europe took a major turn following Russia's invasion of Ukraine. In light of the extensive Western support for Ukraine and the European sanctions policy towards Russia, the likelihood of European countries, and Belgium in particular due to the presence of important international institutions and market infrastructure, being targeted for cyber attacks by either nation-state related groups or so-called "hacktivists" increased sharply. Scenarios in which hackers unintentionally cause collateral damage cannot be ruled out, nor can attacks on critical non-financial infrastructure (telecommunications, energy, etc.), which could have a significant impact on the financial sector. Since the escalation of the geopolitical conflict, the Bank and the financial sector as a whole have demonstrated an increased level of preparedness. Fortunately, thanks to various precautionary measures, this concrete threat did not result in any serious operational incidents during the year under review.

In any case, cyber attacks have already become a daily reality around the world in recent years. Likewise, attackers are continuing to refine the techniques and methods used, making some attacks even more sophisticated, powerful and/or larger in scale. The number of targeted, long-lasting cyber attacks is therefore likely to increase in the future, with the financial sector remaining a potential target. The Carnegie Endowment for International Peace[1] prepares a list of cyber attacks on financial institutions worldwide. This document reveals the current state of cyber threats to the sector. In 2022, reported cyber attacks included the theft of sensitive data, the disruption of systems and the initiation of fraudulent transactions. Reported cases often involved the use of ransomware, distributed denial of service (DDoS) attacks and the exploitation of institutional vulnerabilities, including in supply chains and/or employee gullibility.

1 Timeline of Cyber Incidents Involving Financial Institutions – Carnegie Endowment for International Peace.

Companies and insurance or reinsurance groups are vulnerable to cyber risk on two fronts: on the one hand, they are exposed to cyber attacks as institutions and, on the other hand, they are affected by attacks on their clients, through explicit cover (affirmative cyber insurance) or implicit cover (silent insurance or non-affirmative cyber insurance). Given the increase in the number of cyber attacks during the pandemic and greater public awareness of this possibility, the Bank expects the cyber insurance market to grow rapidly.

In addition to cyber risks, the clear dependence on IT solutions in the financial sector also entails other challenges. Under pressure from innovative actors, increasing customer expectations of services and their availability and increasing (security) risks – for example due to the use of obsolete software which is no longer supported – traditional institutions are being urged to renew their sometimes very old IT architecture in a relatively short time span. However, due to the complexity of their IT environment, it is a challenge to achieve this objective in a responsible manner. There is also a significant risk of increasing dependence on third parties for IT services and other standardised IT system components. In particular, cloud solutions are increasingly being used for ever more important processes. The limited number of critical service providers leads to a growing concentration risk for the financial sector. The potential impact of geopolitical tensions on supply chains has also become very clear in recent years. The need to test software and business recovery solutions sufficiently extensively to cover a range of extreme but plausible scenarios also remains an important focus area.

It is therefore important that the management bodies of financial actors possess the necessary expertise and information to monitor risks appropriately and that they incorporate adequate measures into their strategic planning to keep risks within acceptable limits. However, many institutions report difficulties recruiting staff with the required skills and expertise. Furthermore, all staff of such institutions need to be aware of cyber and IT risks, understand how these can arise and how to react to them.

3.2 Legislative guidelines and developments

In recent years, the Bank has contributed significantly to a regulatory framework aimed at better controlling cyber and IT risks. The circular on the Bank's expectations for the business continuity and security of systemically important institutions remains an important reference. The Bank is also actively contributing to the development of a European regulatory framework for cyber and IT risk management under the auspices of the EBA. This has led to the publication of guidelines for supervisors on ICT risk assessment in the context of the SREP, guidelines on outsourcing, and guidelines on ICT risk and security management. Under the aegis of EIOPA, a comparable regulatory framework has been put in place for the insurance sector in the form of guidelines on outsourcing to cloud service providers and guidelines on ICT security and governance. These guidelines have in the meantime all been incorporated into the Bank's supervision and policy framework. For payment systems and market infrastructure, the ECB's oversight expectations regarding cyber resilience serve as a benchmark. There have also been important developments at the global level. In March 2021, the Basel Committee published new principles to strengthen the operational resilience of banks. One of these principles concerns ICT and cyber security. It goes without saying that these principles are also highly relevant in a digital context.

At the end of 2022, the European Parliament approved a proposal for a regulation on digital operational resilience, called the Digital Operational Resilience Act (DORA). This regulation aims to mitigate the risks associated with the digital transformation of the financial sector by imposing strict common rules on ICT governance and risk management, ICT incident reporting and information sharing, security testing as well as the risk associated with the provision of ICT services by third parties. These rules apply to a wide range of financial institutions as well as to third-party providers of critical ICT services, e.g. cloud service providers, which will be subject to some type of oversight. During the discussions on the draft texts at European level, the Bank played a significant advisory role within the Belgian delegation. It will actively contribute to development of the technical standards that will give shape to the regulation.

Finally, the European Systemic Risk Board published recommendations in early 2022 to create a pan-European framework for the coordination of systemic cyber security incidents. The Bank is also closely involved in the development of these recommendations.

3.3 Operational activities

Assessing and promoting the control of cyber and IT risks is a top priority for the Bank. Cooperation at European and international levels is becoming increasingly important in this regard. In this area, the Bank focuses on the security of and confidence in financial institutions and FMIs, as well as on cross-sectoral strategies to address these risks.

The Bank has adopted a two-pronged approach. On the one hand, institutions that are subject to prudential supervision are required to hold adequate capital to cover their operational risks, which include cyber and IT risks. On the other hand, the operational security and robustness of critical processes of financial institutions and FMIs are closely monitored. The availability, integrity and confidentiality of IT systems and data are important factors in this respect. The Bank carried out several inspections in 2022 (for banks in the context of the SSM) to verify compliance with the regulatory framework and the adequate management of IT systems having regard to cyber and IT risks.

In addition, the Bank monitors these risks in financial institutions and FMIs as part of its ongoing and recurring supervisory activities. In view of the heightened cyber threat resulting from Russia's invasion of Ukraine, the Bank decided in March 2022 to issue several communications to raise awareness of the cyber threat posed by the crisis to the institutions subject to its supervision and to encourage them to improve their operational preparedness. In addition, selected key institutions were invited to complete a short survey. The responses were supplemented by follow-up sessions with the participants. After a thorough analysis of the various responses, the Bank concluded that the sector was generally well informed of the heightened threat level and that it had responded appropriately.

In 2018, the Bank set up a programme for ethical hacking, called TIBER-BE (*Threat Intelligence-Based Ethical Red Teaming Belgium*). The Belgian part of a methodology developed by the Eurosystem, this programme aims, through sophisticated testing, to increase the cyber resilience of financial institutions and FMIs and to provide feedback on the cyber security of the Belgian financial sector as a whole. The Bank encourages these exercises in its capacity as the authority responsible for ensuring financial stability. In 2022, the TIBER-BE framework was updated on the basis of test results and several additional institutions joined. The sector appears convinced of the methodology and added value of these tests.

The Bank is also paying increasing attention to sector-level initiatives. Thus, the SSM regularly conducts cross-sectoral analyses of IT and cyber-related topics. In 2022, for example, all major banks and some smaller banks were asked to complete a questionnaire intended to provide important information for the annual Supervisory Review and Evaluation Process (SREP) on IT aspects and to enable cross-sectoral analyses to be conducted. A large number of insurance undertakings, stockbroking firms, payment institutions and electronic money institutions were also asked to provide the same type of information for a similar purpose.

Also in 2022, a survey was conducted for the first time of selected financial institutions to establish a list of critical third parties that provide them with information and communication technology services. This was a follow-up to an initiative by the European Supervisory Authorities (ESAs), which aimed to get an idea of which third parties could in future qualify as critical service providers under DORA.

In its capacity as the sectoral authority for the application of the law on the security and protection of critical infrastructure (mainly banks and FMIs of systemic importance), the Bank also assesses the effectiveness of control systems in critical financial infrastructure. In this framework it organises and coordinates periodic sector-level crisis simulation exercises, in order to prepare the Belgian financial sector for possible operational incidents of a systemic nature. Under the Networks and Information Systems Security (NIS) Act, the Bank acts as a contact point for major incidents in the sector.

Finally, the Bank participates in various international fora and working groups to better understand the risks that could become systemic for the financial sector and to study mitigation measures. Other initiatives aim to promote the exchange of information between institutions, supervisors, central banks, etc.