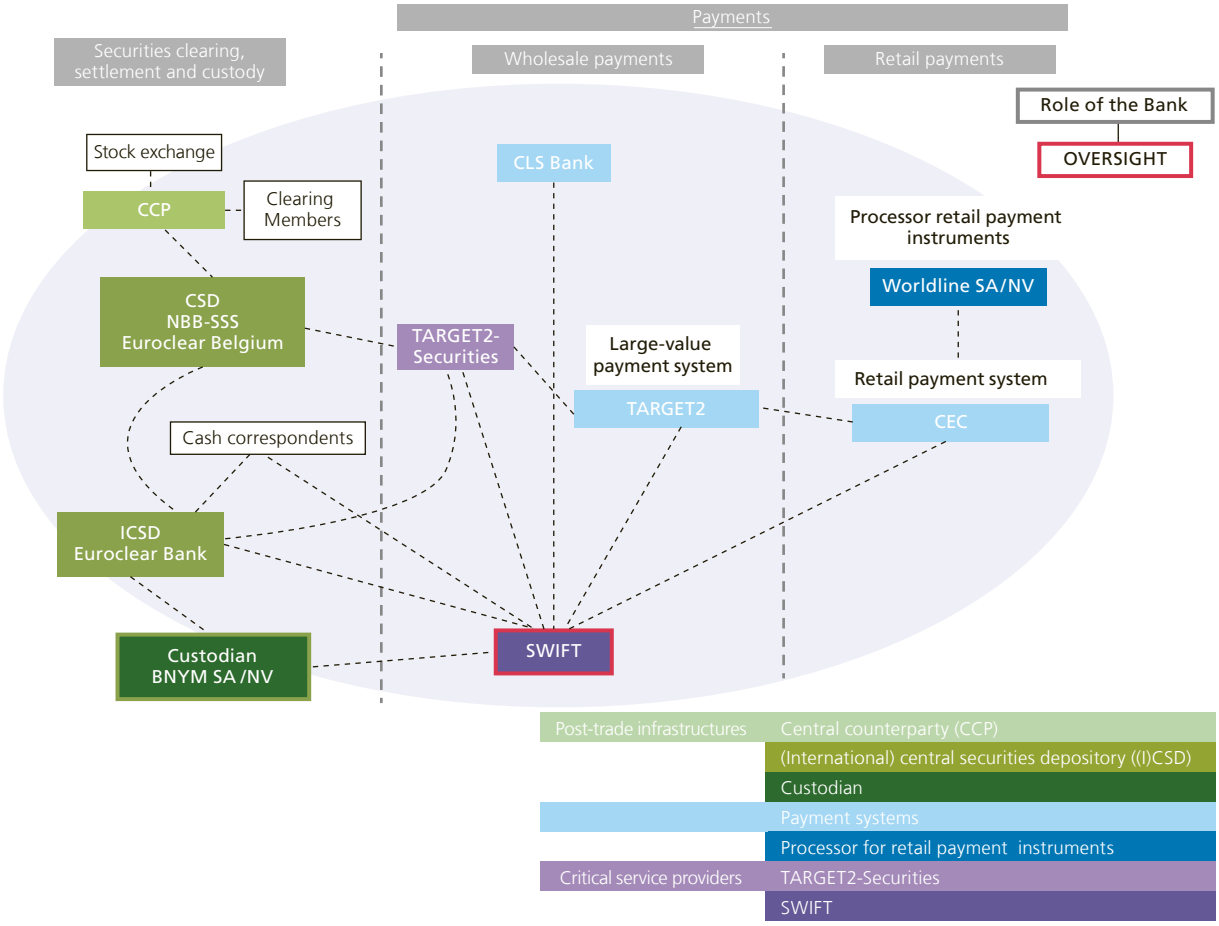
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium that provides messaging and connectivity services to both financial institutions and market infrastructures. These customer types are characterised by their diversity in terms of activities and size, e.g. SWIFT serves banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparties and trusts.

CHART 5 SWIFT AS CRITICAL SERVICE PROVIDER TO THE FINANCIAL INDUSTRY AND THE BANK'S OVERSIGHT ROLE



Source : NBB.

Given its systemic importance as critical service provider to global correspondent banking activities and financial market infrastructures (see chart 5), SWIFT is itself of systemic importance.

Oversight approach

As SWIFT's messaging activities are critical to the smooth functioning, safety and efficiency of major payment and securities settlement systems worldwide (see box 8), the central banks of the G10 agreed to make SWIFT subject to cooperative central bank oversight.

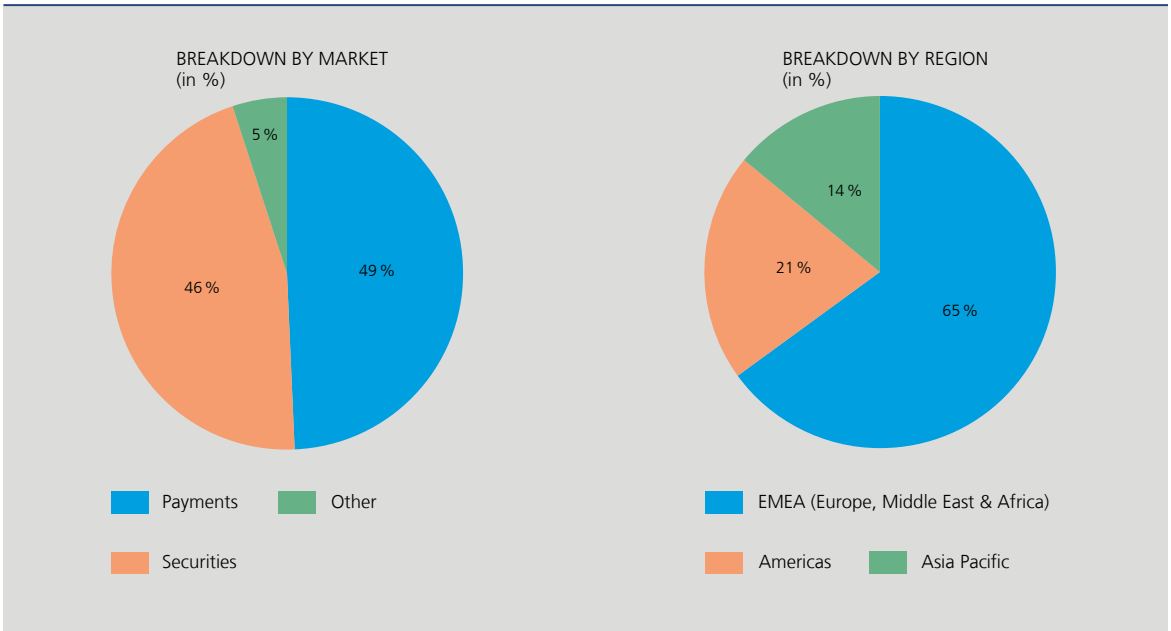
By jointly interacting with SWIFT and formulating joint recommendations concerning it, central banks aim to raise efficiency of their actions as well as the effectiveness of SWIFT's own actions taken in response to their recommendations. Because SWIFT is incorporated in Belgium, the Bank acts as the lead overseer in cooperation with the other G10 central banks. Complementary to this arrangement, a structure is in place to inform the senior overseers from the G20 countries about SWIFT oversight conclusions. The group also discusses oversight policy vis-à-vis SWIFT. An overview of the oversight set-up can be found in box 9.

Box 8 – International dimension of SWIFT

SWIFT is owned and controlled by its members. It has an ongoing dialogue with its customers through national member groups, user groups and dedicated working groups. These discussions relate, for example, to SWIFT's activities such as proposals for new or revised standards, providing industry comments on proposed corporate or business service changes, and comments on timeframes for new technology or service implementation.

SWIFT FIN ACTIVITY

(2017, based on yearly total)



Source: SWIFT.

Each member holds shares proportional to its use of SWIFT's message transmission services. Every three years, a share reallocation is implemented to reflect changes in each member's use of SWIFT. The next reallocation will take place at the 2018 annual general meeting based on 2017 full-year traffic data. Countries or country constituencies propose directors to the Board according to the number of shares owned by all members in the country.

SWIFT's customers are located in more than 200 countries and territories: there are 11 336 live customers of which 2 382 are shareholding members. FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2017 reached 7.08 billion messages (+8.4 % compared to the previous year), i.e. about 28.14 million messages per day. These messages flow between participants in stock exchanges, payment systems, (I)CSDs and CCPs. SWIFT FIN traffic in 2017 was 49 % related to payments and 46 % to securities messaging (see chart below, left-hand panel), The main part of the traffic originated from EMEA members (65 %), followed by those from the Americas region (21 %) (right-hand panel).

Box 9 – The international cooperative oversight of SWIFT

As lead overseer, the Bank conducts the oversight of SWIFT in cooperation with the other G10 central banks (i.e. Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System).

The Bank monitors SWIFT developments on an ongoing basis. It identifies relevant issues through the analysis of documents provided by SWIFT and through discussions with the management. It maintains a continuous relationship with SWIFT, with regular *ad hoc* meetings, and serves as the G10 central banks' entry point for the cooperative oversight of SWIFT. In that capacity, the Bank chairs the senior policy and technical groups that facilitate the cooperative oversight, provides the secretariat and monitors the follow-up of the decisions taken.

The various SWIFT oversight groups are structured as follows:

- the SWIFT Cooperative Oversight Group (OG), composed of all G10 central banks, the ECB and the chairman of the CPMI, is the forum through which central banks conduct cooperative oversight of SWIFT, and in particular discuss oversight strategy and policies related to SWIFT;
- within the OG, the Executive Group (EG) holds discussions with SWIFT's Board and management on the central banks' oversight policy, issues of concern, SWIFT's strategy regarding oversight objectives, and the conclusions. The EG supports the Bank in preparing for discussions within the broader OG, and represents the OG in discussions with SWIFT. The EG can communicate recommendations to SWIFT on behalf of the OG. At one of the EG meetings, the annual reporting by SWIFT's external security auditor is discussed. The EG includes the Bank of Japan, the Federal Reserve Board, the Bank of England, the ECB and the Bank;
- at the technical level, the SWIFT Technical Oversight Group (TG) meets with SWIFT management, internal audit and staff to carry out the groundwork of the oversight. Specialised knowledge is needed to understand SWIFT's use of computer technology and the associated risks. The TG draws its expertise from the pool of staff available at the cooperating central banks. It reports its findings and recommendations to the OG.

The SWIFT Oversight Forum is composed of senior overseers from the G10 central banks (OG) and 10 additional central banks (i.e. Reserve Bank of Australia, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Korea, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank and Central Bank of the Republic of Turkey). Its objectives are to:

- facilitate a coordinated flow of information about SWIFT oversight conclusions to the Forum participants;
- foster discussions on the oversight policy concerning SWIFT;
- provide input to the OG on priorities in the oversight of SWIFT;
- serve as a communications platform on system interdependencies related to the common use of SWIFT or for communication in the event of major contingency situations related to SWIFT.

The framework for the oversight of SWIFT is provided by the five High Level Expectations (HLEs) that focus particularly on the adequate management of operational risks[1]. The framework establishes the common terminology within which oversight discussions can be held. These expectations vis-a-vis SWIFT have evolved into generic oversight requirements for all critical service providers to FMIs, and were included as Annex F in the CPMI-IOSCO Principles for FMIs. SWIFT periodically reports to the overseers on its compliance with the HLEs, which is one of the starting points for identification and further analysis of the risk drivers at SWIFT. Enterprise risk management, information security and technology risk management have been standing topics in the oversight discussions with SWIFT.

Under this framework, the overseers devoted considerable time in 2017 to monitoring SWIFT's Customer Security Programme, and its Global Payments Innovation that aims to increase the transparency and speed of cross-border payment message flows. Overseers also reviewed the expanding portfolio of SWIFT services, e.g. in the area of compliance with financial crime regulation. In the fourth quarter of 2017, the IMF reviewed the SWIFT oversight arrangements in the context of a Financial Sector Assessment Program (FSAP) mission to Belgium (see box 10).

SWIFT's Customer Security Programme aims to strengthen the security of the global financial community against cyber threats by providing guidance to the customers in terms of how they should secure their own local IT infrastructure used for connecting into SWIFT. In addition to this guidance and establishment of a framework to foster increased transparency amongst SWIFT users on customers' adherence to the guiding controls, the programme also focuses on making additional tools available to customers to assist them in preventing and detecting fraud in commercial relationships. Furthermore, under the programme, SWIFT is taking various initiatives for sharing information, thus enabling customers to better prepare for resisting any future cyber threats.

Overseers monitored the significant progress made in 2017 in the first area of the Customer Security Programme ("secure and protect"). In April 2017, SWIFT published its Customer Security Controls Framework introducing a set of mandatory and advisory controls applicable to all customers. After customer consultation and overseers' review, SWIFT explicitly specified – for each control – the objectives and the risks to be addressed. The increased focus on control objectives now allows customers to demonstrate compliance with specific controls through an alternative method, other than the one originally described in the SWIFT controls implementation, as long as the risks identified are mitigated.

All SWIFT customers were required to assess and attest their compliance status against each of the applicable mandatory security controls by the end of 2017. Their self-attestations are collected in a registry that will be used as of 2018 to improve transparency of a SWIFT customer's compliance status vis-à-vis its counterparties. SWIFT customers will be encouraged to take this compliance information into account during their counterparty due diligence reviews. Greater transparency in the SWIFT user community on compliance with security controls is thus a key design feature

(1) The HLEs for the oversight of SWIFT cover (1) risk identification and management, (2) information security, (3) reliability and resilience, (4) technology planning and (5) communication with users.

of the strategy aimed at creating peer-driven pressure to strengthen security. Overseers requested additional security assessments of the registry of attestations itself, and asked SWIFT to consider the development of further action plans if the goals of the current strategy based on transparency amongst customers are not met. Potential issues that need to be monitored might include a limited number of submitted customer attestations and/or low levels of compliance with the controls.

Additionally, SWIFT reserves the right to report customers that did not attest – and, as of January 2019, customers that are non-compliant with the mandatory controls – to their supervisory authority. This escalation process has been reviewed by the overseers.

The overseers also informed SWIFT that they want to be kept informed on relevant metrics to monitor the effectiveness of the customer security controls and attestations. Overseers furthermore continue to follow up on the hardening of the interfaces used by customers to connect to SWIFT, be they installed in their local SWIFT environments or provided by a service provider. They also reviewed the rolling out of SWIFT's Information Sharing and Analysis Centre (ISAC) and the establishment of the Customer Security Intelligence team. Additionally, overseers examined the design and implementation of new financial crime compliance messaging solutions like daily validation reports and payments control and sanctions screening service.

Whereas overseers' monitoring on the further development of the SWIFT Customer Security Programme is inspired by a broad focus on financial stability for the wider ecosystem comprised of SWIFT and its customers, the oversight focus still remains on the security and availability of SWIFT's own operations. Here, too, a major focus is on cyber security matters.

In 2017, the overseers concentrated on the design, implementation and testing of processes for cyber event detection, monitoring and response. Highlights in this area of interest include the review of the multi-year roadmap for further improving the cyber security posture of SWIFT and the review of results of logical intrusion tests and more sophisticated types of penetration testing. Once a year, the overseers also challenge the external security auditor on its opinion and the findings and observations underpinning that opinion.

Interface products for customer connection to SWIFT are not only provided by SWIFT, but also by third parties. Rather than installing such interfaces on their premises, customers can also connect to SWIFT via a service provider (a 'service bureau' or 'shared infrastructure provider'). Overseers not only focused on the Customer Security Programme described earlier, but also reviewed the (cyber) risk mitigation strategies applied by SWIFT to third-party providers of interface products (through a SWIFT certification programme) and shared infrastructure providers. At the request of the overseers, SWIFT aligned the cyber security requirements of the shared infrastructure programme with those of the Customer Security Programme, the latter providing the minimum-security baseline for shared infrastructure. For example, operators of shared infrastructures must comply with both the mandatory and the advisory controls of the Customer Security Programme.

SWIFT's long-term strategy and how it aligns with specific platform investments are regularly discussed with representatives of SWIFT's management and Board. Overseers typically challenge such plans on the aspects of security and strategic focus.

Overseers conduct regular evaluations of the effectiveness of the various lines of defence and governance structures, for daily operations, long-term strategies and specific projects. Specific attention is paid to the development and implementation of the enterprise risk management (ERM) roadmap and the recurring assessment of extreme risks and recovery plans. Overseers are closely monitoring how SWIFT is continuing the build-up of a truly integrated ERM framework that also pays due attention to other types of risk than technical or security risks.

When incidents take place in SWIFT's infrastructure, network or operations, the overseers investigate the sequence of events, analyse the customer impact, and review the results of the investigation. Detailed action plans that outline the activities, deadlines and responsibilities within SWIFT are requested where necessary. There is frequent follow-up on these action plans, designed to prevent recurrence of similar incidents.

Box 10 – IMF recommendations on the oversight of SWIFT

The IMF FSAP mission conducted in the fourth quarter of 2017 in Belgium covered the oversight of SWIFT. The IMF issued three recommendations:

1. Consider a regulatory backstop to complement the current moral suasion basis of the SWIFT oversight;
2. Consider broadening the membership of the SWIFT Oversight Forum;
3. Improve information sharing on SWIFT oversight and assurance reports.

On the first recommendation, legal reviews will be conducted to investigate how moral suasion can be combined with a regulatory backstop. On the expansion of the SWIFT Oversight Forum, contact will be made with additional central banks, inviting them to sign a Memorandum of Understanding with the Bank to join the Forum. The review of criteria determining which central banks will be invited will be discussed with current Forum members. On the increased transparency on SWIFT oversight and SWIFT assurance reports, various initiatives will be undertaken, either by the Bank itself through publications or through meetings and conferences involving relevant stakeholders (e.g. other central banks or financial authorities) or by encouraging SWIFT to make existing assurance reports better known amongst relevant authorities and/or amongst its customers themselves.

Oversight priorities in 2018

The primary oversight focus remains the adequacy of SWIFT's cyber strategy for protecting the infrastructure, networks and operations under its control. This includes the review of the updated multi-year cyber security roadmap and progress in its roll-out. Additionally, the findings – if any – of the external security auditor will be analysed and potential remediation discussed.

Overseers will ask SWIFT to obtain info about relevant metrics to monitor the effectiveness of the Customer Security Programme. Attention will be paid to the level of compliance with the security controls, to validating the current control mix (relevance of current controls, advisory versus mandatory controls), and the effectiveness of the attestation and reporting processes as enforcement mechanisms. When needed, the overseers will request – and review – remediation plans.

These major areas of focus are complemented with continuous monitoring activities structured in line with the HLEs. Firstly, continuous monitoring in the context of the risk identification and management expectations will focus on further development of the ERM methodology and risk acceptance processes, as well as further refinement of the risk registry. The overseers periodically assess the effectiveness of the three lines of defence, i.e. self-assessment of risks by line management, assessments by the independent risk management function, and reviews by internal audit.

Secondly, business continuity processes and disaster recovery strategies will be assessed against the requirements specified in the CPMI-IOSCO guidance on cyber resilience.

Thirdly, overseers plan a series of risk evaluations for strategic IT options and possible future technology renewals. Furthermore, the overseers will review the potential impact of these technology innovations on the confidentiality, integrity and availability of information. Due attention will be paid to review vendor, patching and incident response processes.

Fourthly, the overseers will examine the improvements to the communication processes to inform customers. In the light of recent cyber incidents caused by compromised customer environments, overseers will analyse the functioning of the Customer Security Intelligence team and the distribution of actionable cyber threat information via SWIFT's ISAC.

Additionally, the roll-out of the Customer Security Programme processes for reporting non-compliant customers will be examined and challenged where necessary.

Finally, the overseers continue to analyse the design and follow-up on the implementation of major projects that could significantly impact the risk profile of SWIFT.