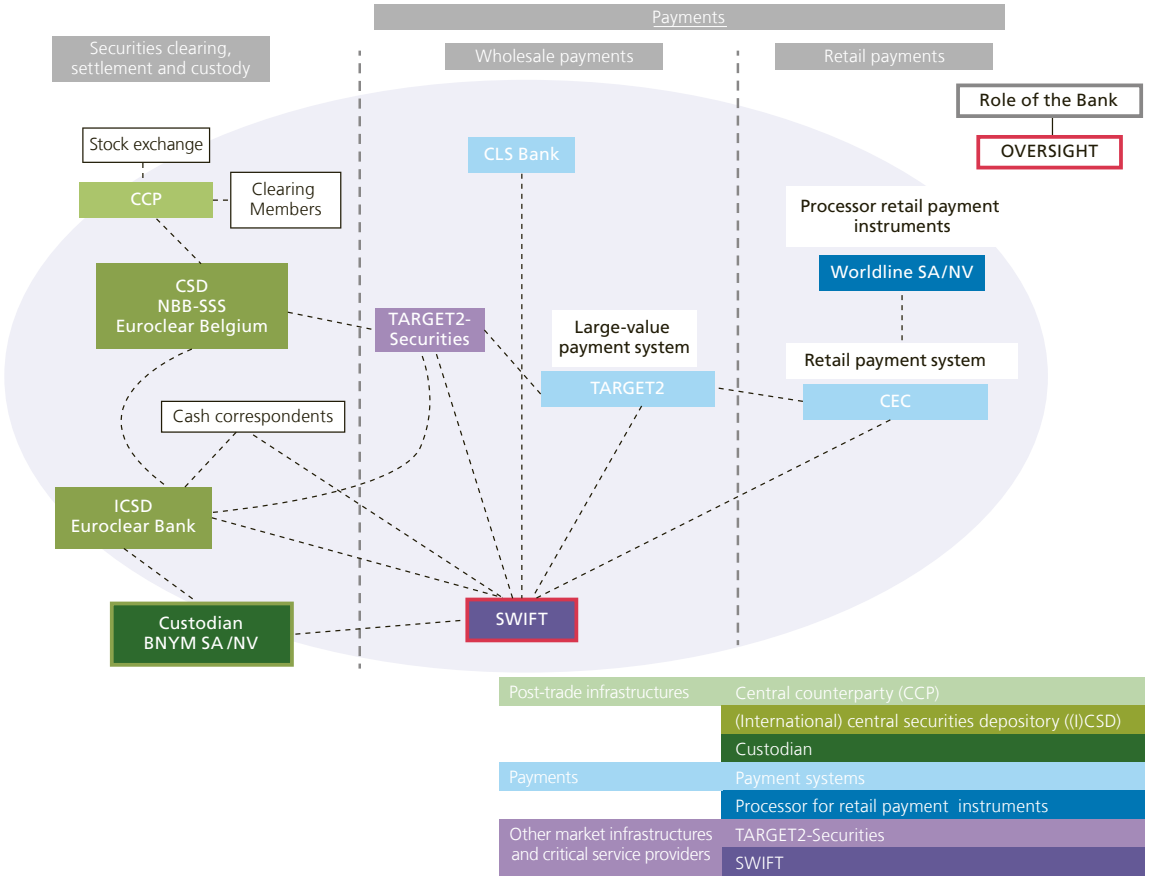
4. SWIFT

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. SWIFT for instance serves banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparties and trusts.

As a critical service provider to systemically important global correspondent banking activities and financial market infrastructures (see chart 5), SWIFT is itself of systemic importance.

Chart 5

SWIFT as a critical service provider to the financial industry and the Bank's oversight role



Oversight approach

As SWIFT's messaging activities are critical to the smooth functioning, safety and efficiency of major payment and securities settlement systems worldwide, the central banks of the G10 agreed to make SWIFT subject to cooperative central bank oversight (see Box 11).

By jointly interacting with SWIFT and formulating joint recommendations concerning it, central banks aim to improve the efficiency of both their own actions and SWIFT's actions taken in response to their recommendations. As SWIFT is incorporated in Belgium, the Bank acts as the lead overseer, in cooperation with the other G10 central banks. To complement this arrangement, the SWIFT Oversight Forum has been put in place to inform the senior overseers from CPMI member countries about SWIFT oversight conclusions. The forum also discusses oversight policy vis-à-vis SWIFT. An overview of the oversight set-up can be found in Box 12.

BOX 11

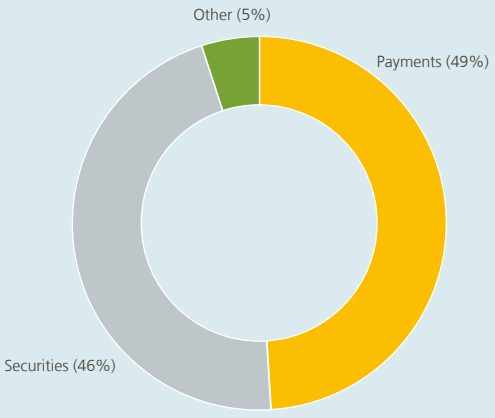
International dimension of SWIFT

SWIFT is owned and controlled by its members. It has an ongoing dialogue with its users 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. Each member holds shares proportional to its use of SWIFT's message transmission services. Every three years, the shares are reallocated to reflect changes in each member's use of SWIFT. The next reallocation will take place at the 2021 annual general meeting. Countries or country constituencies propose directors to the Board according to the number of shares owned by all members in the country.

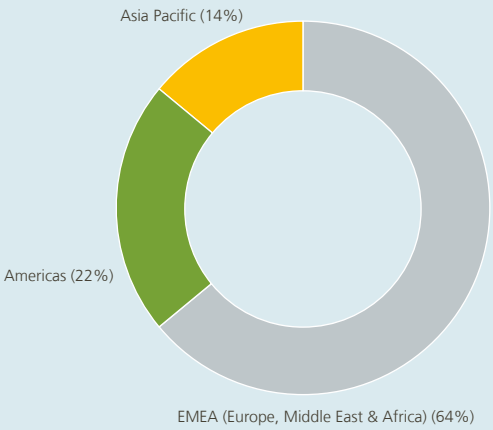
SWIFT FIN activity

(2018, based on yearly total)

Breakdown by market



Breakdown by region



Source: SWIFT.

SWIFT's customers are located in more than 200 countries and territories: there are 11 324 live users, 2 440 of whom are shareholding members. FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2018 reached 7.9 billion messages (+11.3 % compared to the previous year), i.e. about 31.3 million messages per day. These messages flow between participants in stock exchanges, payment systems, correspondent banking, (I)CSDs and CCPs. In 2018, 49 % of SWIFT FIN traffic related to payments and 46 % to securities messaging (see chart below, left-hand panel), The main part of the traffic originated from EMEA members (64 %), followed by members from the Americas region (22 %) (right-hand panel).

BOX 12

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 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 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. The EG discusses the annual reporting by SWIFT's external security auditor at one of its meetings. 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 for 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 15 additional central banks (i.e. Central Bank of the Argentine Republic, Reserve Bank of Australia, Banco Central do Brazil, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Indonesia, Bank of Korea, Bank of Mexico, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank, Banco de España and Central Bank of the Republic of Turkey)[1]. 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 platform for communication on system interdependencies related to the common use of SWIFT or for communication in the event of major contingency situations related to SWIFT.

1 Following the IMF's recommendation to consider a further broadening of the membership of the SWIFT Oversight Forum, its membership was aligned with the composition of the CPMI. Central Bank of the Argentine Republic, Banco Central do Brazil, Bank of Indonesia, Bank of Mexico and Banco de España joined the SWIFT Oversight Forum in 2019.

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. This reporting serves as one of the starting points for identification and further analysis of the risk drivers for 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 2018 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. to detect wholesale payment fraud.

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.

Customer security programme

SWIFT's Customer Security Programme aims to strengthen the security of the global financial community against cyberthreats by providing requirements for customers in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT. In addition to this guidance and the establishment of a framework to foster increased transparency amongst SWIFT users on customers' adherence to the 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 takes various initiatives for sharing information, thus enabling customers to better prepare for resisting any future cyberthreats. Progress is monitored against the CPMI wholesale payment fraud prevention, detection, reaction and information sharing strategy, which is described in Box 13.

Overseers review the evolving security requirements for customers' local IT infrastructure to obtain reasonable assurance on their effectiveness in reducing the risks for SWIFT, its participants and community. An important oversight objective is to ensure that these security requirements continue to evolve in line with emerging threats, advances in cybersecurity practices and regulatory developments.

SWIFT's Customer Security Control Framework outlines the set of mandatory and advisory security controls for customers' local IT infrastructures. Mandatory security controls establish a security baseline to which all SWIFT users must adhere, whereas advisory controls describe good practices for securing local IT infrastructures.

In 2018, SWIFT presented the first revision of its Customer Security Control Framework. With this revision, SWIFT raises the security baseline by promoting three optional security best practices to mandatory requirements for the customers' local IT infrastructure. With the introduction of two additional advisory controls, SWIFT further extended its set of good practices for the customers' local IT infrastructure. Furthermore, SWIFT clarified the implementation guidelines for multiple customer security controls. The overseers ratified the proposed changes prior to publication and communicated their vision on future evolutions (including the importance of reliable fraud detection and prevention tools).

SWIFT committed to periodically improve the Customer Security Control Framework following a standardised change management strategy, which has been evaluated and accepted by the overseers. With transparent and standard adoption timeframes, SWIFT aims at improving the predictability of the process enabling participants to timely plan and budget additional measures needed to comply with the proposed updates. Change requests are captured through interaction with different stakeholders, including the overseers, SWIFT's participants and their supervisors, and cybersecurity experts. SWIFT does reserve the right to issue an emergency update to address extreme developments in the threat landscape, as strictly requested by the overseers.

All SWIFT users were required to re-assess and attest their compliance status based on each of the applicable mandatory security controls by the end of 2018. SWIFT reported an important uptake of the self-attestation process, self-attesting institutions covering more than 99 % of all FIN messages sent over the SWIFT network. The major oversight concerns in this context relate to ensuring continued customer engagement in the attestation process, participants' compliance with the evolving set of mandatory controls and the veracity of submitted self-attestations. In response to overseers' requests, SWIFT proposed an independent assurance framework covering both audit methodologies and assurance requirements.

Customers are encouraged to consult the self-attested information of their counterparties to obtain insight into their security posture and take appropriate risk mitigation measures, in order to create peer pressure to strengthen security across the ecosystem. To support this process, SWIFT introduced enhanced functionalities for the self-attestation registry (including bulk access requests and auto-grant functionality) and guidelines on including self-attestation information in counterparty risk assessments. Overseers continue to monitor the self-attestation and consultation process, as well as the level of compliance with the mandatory security controls, across different customer segments.

As of January 2019, SWIFT reserves the right to report users who have failed to timely self-attest full compliance with all mandatory security controls or who depend on non-compliant service providers (a "service bureau" or "shared infrastructure provider"), to their local supervisors. Participants must re-attest at least every twelve months and within a month after self-attestations have proven to be inaccurate (e.g. changes to the infrastructure or findings by independent assurance providers). Self-attestation information, especially information regarding non-compliance or compliance downgrades after the identification of inaccuracies by independent reviewers, could be an important input for these supervisory authorities' risk-based planning and the scoping of supervisory inspections.

The overseers requested SWIFT to report quality assurance metrics that enable an assessment of the attestation, consultation and reporting processes' effectiveness, as well as of the security gains obtained across the different participant types. Quality assurance metrics are continuously being refined and extended by the overseers to improve their monitoring activities. Based on the reported metrics, SWIFT overseers determine whether and what additional oversight demands need to be formulated.

Furthermore, overseers continue to review the adequacy of SWIFT's interface hardening and its adoption rate by SWIFT users, to examine the continuous improvement of SWIFT's Information Sharing and Analysis Centre (ISAC), to encourage reaching out to smaller users and fostering the further development of the Customer Security Intelligence team. In the context of recurring SWIFT service reviews, the overseers examined the design and implementation of new financial crime compliance messaging solutions that aim at combatting wholesale payment fraud like the Payment Control Service.

Standing oversight activities in 2018

Whereas overseers' monitoring of 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 remains on the security and availability of SWIFT's own operations. Here too, the major focus is on cybersecurity matters.

In 2018, the overseers focused on the design, implementation and testing of cyberevent detection, response and recovery measures. The multi-year roadmap for further improving the cybersecurity posture of SWIFT has been reviewed, as well as assessed against the evolving threat landscape and identified technology risks. Furthermore, the overseers reviewed the scope and attack vectors used in the logical intrusion tests, as well as the implementation of the related action plans. Every year, the overseers also challenge the external security auditor' opinions and findings.

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 and shared infrastructure providers.

SWIFT's long-term strategy and how it is aligned with specific platform investments are regularly discussed with representatives of SWIFT's management and Board. Overseers typically challenge the security and strategic focus of such plans. Additionally, the overseers reviewed SWIFT's Board of Directors ISO20022 study and migration plan.

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. In 2018, the overseers conducted an in-depth review of the continued development of a truly integrated enterprise risk management (ERM) framework that pays due attention to other types of risk than technical or security risks (e.g. business, legal, people and third-party risk). In addition to the ERM framework's design, the overseers analysed its implementation and the interaction with SWIFT's management and Board of Directors.

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. These action plans are frequently followed up, in order to prevent recurrence of similar incidents.

BOX 13

CPMI Strategy for reducing the risk of wholesale payments fraud related to endpoint security

In May 2018, the Basel Committee on Payments and Market Infrastructures (CPMI) presented a strategy to encourage and help focus industry efforts towards reducing the risk of wholesale payments fraud related to compromised customer IT infrastructures [1]. Governors of the BIS Global Economy Meeting (GEM), i.e. the Governors of 30 BIS member central banks in major advanced and emerging market economies that account for approximately four fifths of the global GDP, expressed their support and commitment for operationalising the strategy within their institutions and jurisdictions.

The **strategy** aims at exhaustively addressing the areas relevant to payment fraud prevention, detection, response and (external) communication. Seven strategy elements provide a high-level overview of the actions needed.

1. Identify and understand the range of risks;
2. Establish endpoint requirements;
3. Promote adherence;
4. Provide and use information and tools to improve prevention and detection;
5. Respond in a timely way to potential fraud;
6. Support ongoing education, awareness and information-sharing;
7. Learn, evolve and coordinate.

While being descriptive and thereby allowing for the necessary flexibility, the CPMI has distilled points for consideration from experienced stakeholders' comments. These points for consideration could assist other operators, participants and relevant stakeholders in developing and operationalising their individual security strategy.

1 https://www.bis.org/cpmi/publ/d178.htm.

All stakeholders in the wholesale payment ecosystem should take responsibility for their own systems, risk management and internal control frameworks. Concretely, complying with endpoint security requirements does not imply a shift in liability from participants to wholesale payment system or network operators; participants remain responsible for conducting adequate due diligence assessments of counterparties; and participants adopting fraud prevention and detection tools developed by a payment system or network operator remain responsible for accurately parameterising these tools and dealing with the alerts that they generate.

A successful **operationalisation** of the presented strategy will depend on the active cooperation between all relevant actors, including payment system operators, participants and public stakeholders. The CPMI is committed to promoting effective and coherent operationalisation of the strategy within and across jurisdictions and systems. CPMI member central banks will act as a catalyst for the effective and coherent operationalisation of the strategy within and across jurisdictions and systems, monitor progress throughout 2018 and 2019, and where necessary take action to ensure adequate progress in the operationalisation of the strategy.

In February 2019, the CPMI organised a workshop with participants from the different stakeholders in the strategy operationalisation. Emerging practices as well as challenges faced by the different stakeholders were shared. Several multilateral groups that could assist in advancing the implementation and addressing the challenges were identified. CPMI members continue their efforts to outreach to non-CPMI central banks, regional associations and bank supervisors.

The strategy is relevant for several risk management topics covered in the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), Annex F of the PFMIs on oversight expectations for critical service providers and the CPMI-IOSCO guidance on cyberresilience for financial market infrastructures. It is not intended to replace or supersede them.

Oversight priorities in 2019

The primary oversight focus remains the adequacy of SWIFT's cyberstrategy to protect the infrastructure, networks and operations under its control. This includes a review of the updated multi-year cybersecurity 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 continue to monitor relevant metrics to monitor the effectiveness of the Customer Security Programme and request the specification of additional measures where needed. Focus will be placed on the level of compliance with the security controls, the continued appropriateness of the mandatory control set in a changing environment, the effectiveness of the adherence promotion mechanisms (i.e. assurance, attestation and reporting processes) and the reach out to the different stakeholders. Special attention will be paid to SWIFT's proposals to improve the communities' confidence in the veracity of the submitted self-attestations.

These major areas of focus are complemented with continuous monitoring activities structured in line with the HLEs.

Firstly, overseers periodically assess the effectiveness of the three lines of defence (i.e. SWIFT's management, independent risk management function and internal audit function) in adequately identifying, assessing and mitigating specific risks. Due attention is paid to the further development of the ERM methodology and risk acceptance processes.

Secondly, SWIFT's business continuity management framework and disaster recovery strategies are periodically assessed against the requirements specified in the CPMI-IOSCO guidance on cyberresilience. Within this context overseers will focus on SWIFT's extreme cyberrisk scenario assessment and its progress towards the achievement of the 2-hour recovery time objective (2h RTO).

Thirdly, overseers continue assessing the risks related to strategic IT options and possible future technology renewals regarding information confidentiality, integrity and availability. Special attention will be paid to SWIFT's third party vulnerability management and incident response processes.

Fourthly, the overseers will examine the improvements to the communication processes used to inform users. The 2019 oversight priorities in this context are the communication regarding security updates (including release 7.3), the customer security programme (including communication to smaller participants, the functioning of the Customer Security Intelligence team and the distribution of actionable cyberthreat information via SWIFT's ISAC) and the customer involvement in business continuity testing.

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