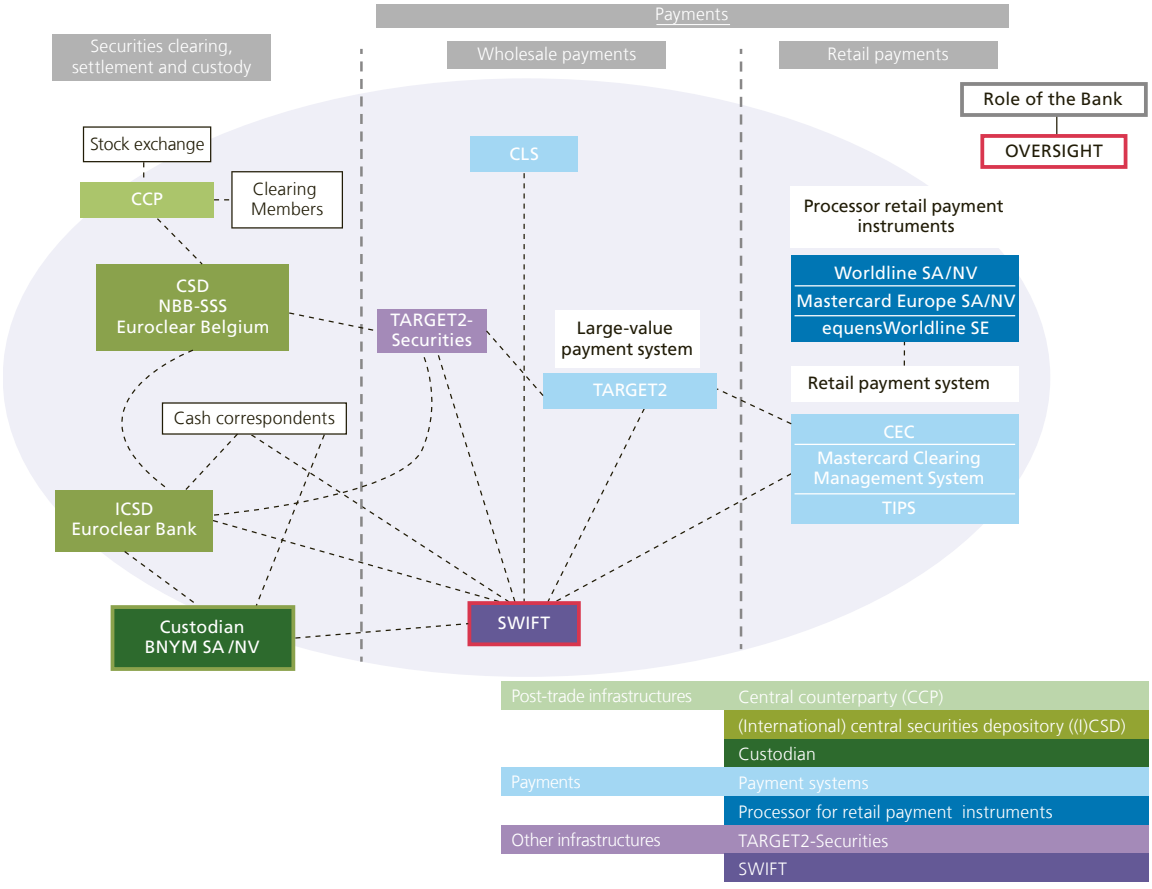
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides global messaging and connectivity services to various financial institutions and market infrastructures, such as banks, brokers, investment managers and other. SWIFT is a limited liability cooperative company registered in Belgium and has its headquarters in La Hulpe.

Correspondent banking activities and financial market infrastructures systemically depend on SWIFT for its financial messaging. SWIFT thus plays a fundamental role in the global financial industry and acts as a critical service provider to the financial institutions and market infrastructures (see chart 4). For this reason, the G10 central banks have classified SWIFT as systemically vital and established the cooperative central bank oversight on SWIFT.

Chart 4

SWIFT as a critical service provider to the financial industry



4.1 Oversight approach

At the end of 1997, a formal set-up of the oversight on SWIFT was established by the G10 central banks[1]. At the heart of this formalised structure lies the international cooperative arrangement conducted by the G10 with the objective of overseeing the adequate and safe functioning of SWIFT. Since SWIFT is based in Belgium, the National Bank of Belgium holds the mandate of lead overseer and chairs the international oversight meetings.

International dimension

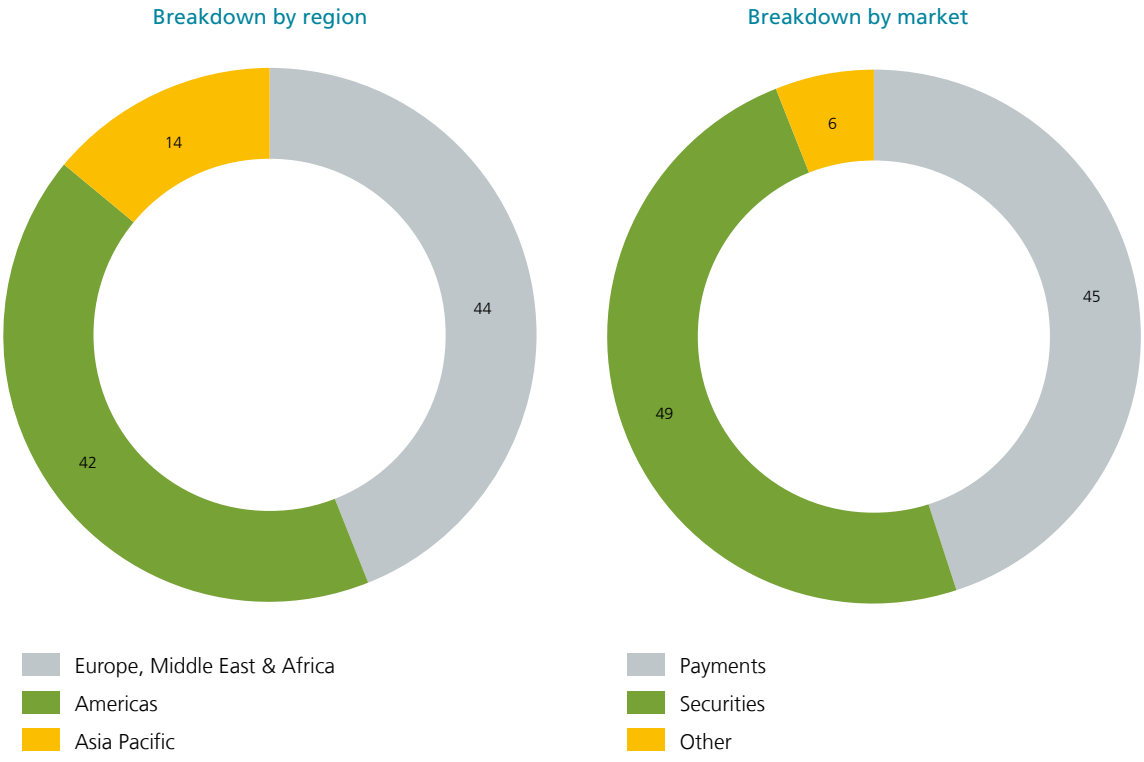
SWIFT operates in an international context with activities spread over more than 200 nations. This is illustrated by the company's messaging volumes: in 2020 9.5 billion messages (+10.3 % compared to 2019) were sent with an average of 37.7 million messages per day.

SWIFT is owned and controlled by its users, who are organised in national member groups, user groups and dedicated work groups. It arranges frequent touchpoints with these different parties to ensure continuous dialogue and timely updates on strategy or product developments. The industry-specific work groups cover various topics for discussion between SWIFT and its users, for example security hardenings of its interfaces, new

1 The G10 central banks involved in the SWIFT oversight are 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.

Chart 5

SWIFT FIN activity



Source: SWIFT.

technology implementations, messaging service changes. An example of such a dedicated work group is the Payments Market Practice Group[1].

The message traffic over SWIFT's network determines the company's share distribution. As a result, the shares are reallocated every three years in order to more realistically mirror the SWIFT messaging user community. SWIFT Board members are appointed by the countries or country constituencies based on the number of shares owned by all users in the respective jurisdiction. The previous redistribution took place in 2018, which means that one will take place during this year's annual general meeting. The next share revision is scheduled for 2024.

SWIFT's FIN traffic for 2020 per market and region is illustrated by the following two charts. FIN is SWIFT's core messaging service for sending and receiving financial messages. There are 11 588 live users of whom 2 372 represent shareholders. As in previous years, the 2020 payments (45 %) and securities (49 %) messaging represent the largest categories. The Europe, Middle East & Africa region has the largest share (44 %) of the total 2020 FIN traffic volume.

International cooperative arrangement

The central banks that roughly represent the G20 countries[2] are directly involved in the international cooperative oversight of SWIFT. This arrangement is formalised in a framework which sets out the role of the NBB as lead overseer, and the scope and frequency of the different oversight work groups.

The NBB's role as lead overseer consists of the daily monitoring and follow-up of SWIFT's activities and projects. Depending on the topic, frequent bilateral interactions take place between SWIFT's three lines of defence[3] and the NBB oversight team. The information relevant to the other overseers is shared in order to ensure a transparent cooperative oversight with the other central banks. The relationship between SWIFT and the NBB is defined via the SWIFT Oversight Protocol. The NBB also integrates another main activity in its mandate as lead overseer, namely the coordination and organisation of the different international workgroups it chairs. In that capacity, the NBB oversight team also drives the SWIFT oversight outreach activities to other stakeholders, such as the central banks that are not directly involved in these oversight activities.

There are four work groups defined in the oversight framework : Cooperative Oversight Group (OG), Executive Group (EG), Technical Group (TG) and SWIFT Oversight Forum (SOF). Each group has a specified scope and frequency of interaction. In addition, touchpoints exist between the different groups and with SWIFT. The SWIFT oversight relationships between the SWIFT overseers and the NBB are laid down in a Memorandum of Understanding (MoU). The following paragraphs provide more detail on the different oversight bodies.

The Cooperative Oversight Group (OG) is represented by the G10 central banks and the chairperson of the CPMI. Each G10 central bank appoints a senior-level overseer to participate in the two annual meetings. OG members decide on SWIFT oversight planning, conclusions, policies and recommendations to SWIFT. Throughout the year, there are also *ad-hoc* interactions scheduled with the OG members when certain developments at SWIFT require additional review.

The OG decisions and recommendations are communicated to SWIFT in the Executive Group (EG) meetings that typically take place after the OG meeting and after a SWIFT Board meeting. Each year, three EG meetings take place in order to better align with the OG meetings and to ensure SWIFT shares information with overseers on SWIFT Board decisions and developments in good time. The EG consists of a sub-set of the OG members which

1 SWIFT established the Payments Market Practice Group (PMPG) to facilitate the ISO 20022 global migration. The PMPG consists of market infrastructure and bank representatives.

2 The G20 countries directly involved in SWIFT oversight are represented by the G10 central banks 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).

3 The three lines of defence traditionally represent the first line that owns and manages risk, the second line that oversees and challenges the first line's risk management, and the third line that is responsible for independent assurance.

represent the four major global currencies, i.e. NBB as chair, Bank of Japan, Bank of England, European Central Bank, and Federal Reserve Board of Governors. Overseers communicate the OG decisions and recommendations directly to the SWIFT delegation, consisting of the SWIFT Executive Management and Board members.

The G10 Technical Group (TG) conducts the technical fieldwork of SWIFT developments and projects, and reports directly to the OG. Four meetings are planned each year, which include foreseen interactions with SWIFT management, internal audit and independent risk functions in order to carry out the deeper technical oversight analysis. Skills and knowledge on technological and IT-specific domains are required to better understand these developments and their accompanying risks within SWIFT.

The SWIFT Oversight Forum (SOF) represents a wider group of countries based on their share in the total SWIFT traffic volume and in alignment with the CPMI membership composition. The SOF consists of the G10 OG senior-level overseers 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). The SWIFT oversight conclusions, planning and priorities are shared with the SOF. Furthermore, the SOF provides input to OG discussions and serves as a platform for communication on system interdependencies related to the use of SWIFT in their jurisdictions. The NBB continuously seeks ways to improve its outreach to other central banks, as is depicted in the following box.

BOX 10

Involving the central bank community

SWIFT's critical and systemic nature to the financial industry and the 2018 IMF recommendations to further extend the sharing of oversight information to the wider central bank community resulted in the strengthened involvement of the SOF and in the organisation of outreach activities.

In 2012, the G10 Technical Group (TG), Oversight Group (OG) and Executive Group (EG) were supplemented with the SWIFT Oversight Forum (SOF). The SOF enables information-sharing on SWIFT oversight activities with a wider group of central banks. In line with the expansion of the Committee on Payments and Market Infrastructures (CPMI), new members were invited to join the SOF in 2019: Argentina, Indonesia and Spain. At the same time, pending invitations for Brazil and Mexico were updated.

The key objectives as specified in the SOF Terms of Reference are the following:

- facilitate a coordinated flow of information about SWIFT oversight conclusions to the Forum participants;
- foster discussions on the oversight policy directed to SWIFT;
- provide input to the SWIFT Cooperative Oversight Group 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 case of major contingency situations related to SWIFT.

With the aim of continuously widening information-sharing, it has been decided to involve the SOF members more actively in Customer Security Programme (CSP) topics. A larger number of central banks

play an important role to reach out on CSP either to other authorities (e.g. bank supervisors) or to other jurisdictions beyond the SOF countries or through regional outreach initiatives.

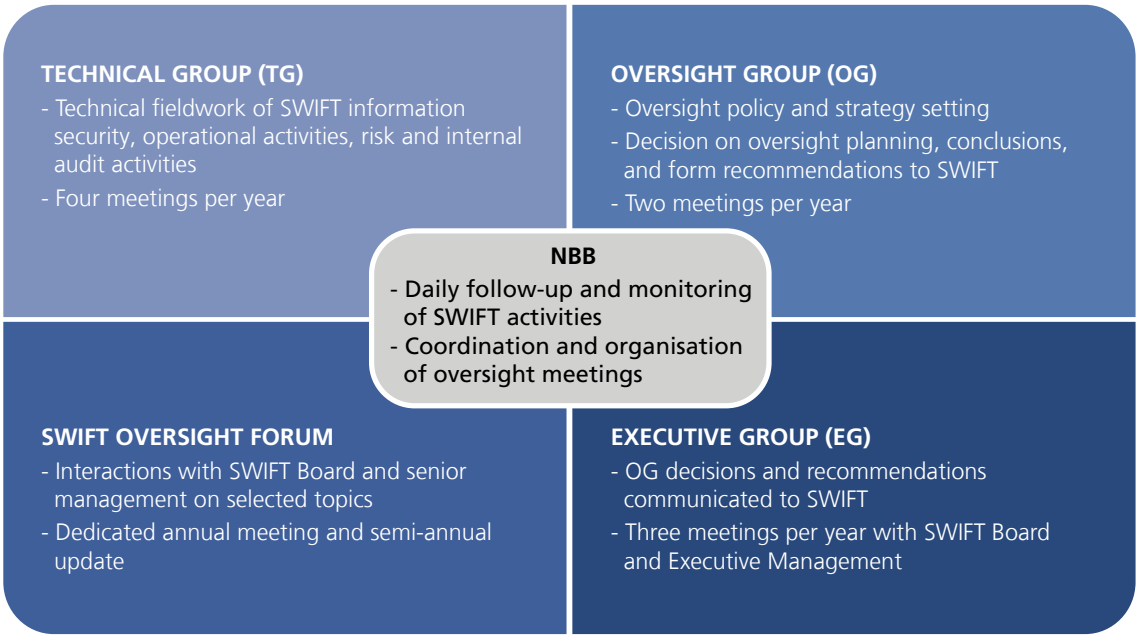
The NBB has organised such regional initiatives on previous occasions. The first regional outreach session took place in 2018 during SWIFT's Sibos conference. The aim was to interact and engage with both the directly involved SWIFT overseers and the non-G20 central bankers on SWIFT oversight topics, such as oversight conclusions, priorities, major SWIFT developments, possible impact on users, and the importance of the role of the SWIFT community. Such outreach sessions during SWIFT's international conference have multiple advantages : a large and globally widespread delegation attends Sibos, each year Sibos is located in another continent, and the majority of the Sibos participants are senior central bank representatives and directors of payments, IT and FMI oversight departments. The second outreach session took place during the 2019 Sibos event, attracting about 70 participants from more than 50 different countries.

A third regional outreach session was planned during the 2020 Sibos conference. Unfortunately, this had to be cancelled because of the COVID-19 pandemic outbreak. SWIFT re-arranged its physical event into a digital Sibos, which made it impractical to organise the foreseen oversight outreach session.

As one of the standing SOF members, the Monetary Authority of Singapore and the NBB planned to jointly hold an outreach session in February 2020 to interact with central banks and supervisory authorities from South-East Asia on relevant SWIFT oversight activities. However, this planned meeting also had to be postponed as a result of the global pandemic but will be rescheduled when circumstances allow.

The following figure gives an overview of the different workgroups involved in the SWIFT oversight.

Cooperative Oversight of SWIFT through different international workgroups



The work group organisations mentioned in the above figure had to be reshuffled because of COVID-19. The planned physical meetings in 2020 were switched to multiple virtual meetings in order to execute and finalise the foreseen planning of oversight activities. The next box provides more information as to what extent COVID-19 impacted SWIFT's oversight work.

BOX 11

COVID-19 impact on oversight activities

The COVID-19 virus spread globally in a sudden and unexpected manner. Therefore, overseers had to logistically rearrange their SWIFT oversight activities. Traditionally, multiple physical meetings with the other central bank overseers are organised throughout the year. The crisis situation forced authorities to restrict travelling, which led to the cancellation of physical oversight and outreach meetings. Nevertheless, the overseers continued their critical review on SWIFT in a decentralised manner in order to cover planned areas such as cyber security, Enterprise Risk Management, Customer Security Programme, and Internal Audit topics. In addition, the COVID-19 implications for SWIFT became a recurring topic for discussion and analysis in the different workgroups.

The OG, EG, TG and SOF meetings all took place virtually in 2020. The four TG meetings were replaced by a series of conference calls aligned with the initially foreseen 2020 oversight planning. As it became clear that the COVID-19 situation would persist until at least the end of 2020 with generalised working from home, the TG refocused its activities around three main guiding principles:

- operational risks, both general and pandemic-related, require close monitoring (e.g. cybersecurity strategy):
- critical business, technology and IT projects must be reviewed (e.g. ISO 20022 migration):
- assurance on the effectiveness of the three lines of defence needs to be obtained.

On top of the conference calls and as a standard work practice, the TG also analysed the extensive documents provided by SWIFT. Follow-up items were identified and communicated over written procedure and conference calls.

On-site reviews have been recently added to the SWIFT oversight toolbox in order to gain additional and deeper knowledge on certain SWIFT domains for which the current oversight structure foresees limited possibilities. In 2018, an extensive on-site review took place on SWIFT's Enterprise Risk Management. In view of the insight gained, the overseers decided to organise a second review in 2020 on cyber security. The initially planned review in the first quarter of 2020 had to be postponed owing to visitor restrictions at SWIFT imposed at the beginning of the pandemic, international travel restrictions and other uncertainties. Eventually, the on-site review team decided to carry out the scheduled review on cyber security through a decentralised approach. Instead of the physical interactions with SWIFT, the review took place over a series of virtual meetings at the end of 2020 to finalise the foreseen activities.

Thanks to the possibility of organising the SWIFT oversight meetings digitally, the pandemic generally did not blur the 2020 oversight priorities and overseers continued to adequately assess SWIFT's activities from a cyber and operational risk-based view.

Oversight expectations

SWIFT oversight risk-based activities are focused around the five High-Level Expectations (HLEs): (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with Users. Through these expectations, overseers assess SWIFT's adequacy of managing operational and technology risks. The HLEs form the basis for the oversight planning, discussions and priority setting. These five expectations evolved into generic oversight requirements for all critical service providers to FMIs and are formalised in Annex F of the CPMI-IOSCO Principles for FMIs.

Overseers expect SWIFT to be in accordance with the five HLEs. This is assessed through different channels: bilateral discussions between NBB and SWIFT, frequent TG interactions with SWIFT's three lines of defence, interactions with SWIFT senior management at OG and SOF meetings, interactions with SWIFT Board and senior management at EG meetings, and through analysing documentation provided by SWIFT. SWIFT's reporting to overseers serves as input for oversight follow-up and gives also an indication of the risk drivers for SWIFT. Standing topics in the oversight analysis are ERM, information security, technology implementation and risk management.

4.2 Covered oversight topics in 2020

Overseers seek to obtain assurance that the corresponding risks in the domains as listed in the five HLEs are adequately assessed, monitored and mitigated in contemplation of the reliability of SWIFT's services. An important topic for overseers is the SWIFT Customer Security Programme (CSP), which received extensive attention from overseers in 2020. Other major projects, such as the planned ISO 20022 migration for cross-border payments and cash management have been included in the overseers' review. The COVID-19 pandemic implied an additional oversight attention point. Overseers assessed its impact on SWIFT's projects, operations, security and resilience, and also the adequacy of SWIFT's response and mitigating actions to the new emerging risks and challenges caused by the pandemic.

Customer Security Programme (CSP)

Since the cyber threat to the financial industry has not diminished, overseers continued to review the effectiveness and further maturing of the CSP in 2020. In the aftermath of the 2016 Bangladesh cyber heist, SWIFT launched the CSP. Through this Programme, SWIFT endeavours to enhance the cyber security in its user community and wider financial industry against potential hackers. The CSP sets out certain requirements how users are expected to adequately secure their on-premise IT components that connect to SWIFT's secure network.

The Customer Security Control Framework (CSCF) has been analysed by overseers on the effectiveness of the implementation and reporting processes. The CSCF consists of a set of mandatory and advisory controls. SWIFT users are expected to be compliant with the mandatory security controls which set a security baseline. The advisory controls are also applicable to all SWIFT users but describe rather good practices for securing local IT infrastructures. A SWIFT user is encouraged to also be in accordance with these advisory controls. A user's compliance is reported through a self-attestation to the framework, which is uploaded through SWIFT's Know Your Customer – Self Attestation (KYC-SA) tool by the end of each year.

By 31 December 2020, 89 % of customers had submitted their attestation for the mandatory controls. The number of self-attestations for 2020 shows a similar uptake compared to 2019. SWIFT provides overseers with quality assurance and monthly metrics reports, which contain an overview of the attestation levels, consultation, reporting processes' effectiveness, and the security advances across different user types. Overseers actively analyse these reports provided by SWIFT. In order to improve the monitoring capabilities, overseers assume SWIFT will refine and extend the CSP reporting metrics. In 2020, a dedicated CSP working group had been temporarily

established with overseers and SWIFT representatives to carry out an in-depth review as to how SWIFT could better meet overseers' expectations on CSP reporting.

Each year, SWIFT publishes a new version of its CSCF. In 2020, it prepared CSCF v2021 which was published in mid-2020 and with which users are expected to be compliant with by the end of 2021. Before SWIFT formally implements the new framework version, a consultation process is planned which involves two main external stakeholders: the user community and SWIFT overseers. For the user community, SWIFT collects feedback through the National Member Groups. As second main stakeholder in the yearly recurring consultation process, overseers have the possibility to provide input to SWIFT's suggested CSCF version adaptations of mandatory and advisory controls. Other stakeholders involved in the consultation process are cyber security experts and supervisory authorities. To reduce the operational burden on its participants in context of the pandemic, SWIFT included limited changes in CSCF v2021: one advisory control, which was part of a mandatory control in previous framework versions, was promoted to mandatory. Multiple existing controls received clarifications on their implementation.

In 2020, overseers also followed up on the enhanced role for supervisory authorities, more specifically on SWIFT's initiatives to onboard supervisors to SWIFT's Know-Your-Supervisor (KYS) tool. Through the KYS tool, supervisors will be able to retrieve self-attestation data of financial institutions in their jurisdiction. The self-attestation information could serve as an important input for risk-based planning and scoping for supervisory authorities. SWIFT reserves the right to report to the competent supervisory authorities those users who have failed to self-attest full compliance with all mandatory CSCF controls in time or users who depend on non-compliant service providers.

The requirement for all SWIFT users to complement their self-attestations with an independent assessment conducted by internal or external auditors was initially planned to kick off in 2020, but the pandemic complicated implementation (e.g. restricted physical inspections). After the overseers' review, SWIFT ultimately decided to postpone the launch of the Independent Assessment Framework, as part of its mitigating CSP actions. The box on "mitigating initiatives taken by SWIFT" in the next paragraph on COVID-19 highlights the CSP and other mitigating initiatives SWIFT considered as a result of the crisis.

The consultation process, in which a user has the possibility of using information from their counterparties' CSCF self-attestations, was also followed up by overseers in 2020. SWIFT proposed improvements to this process to stimulate peer pressure of improving a user's counterparties' risk-mitigating measures and security position. SWIFT further enhanced the KYC-SA functionality to ensure that counterparties have access to more actionable information and smoothened the consultation functionalities. Overseers will continue their review on this process and SWIFT's proposed improvements.

Overseers also include in their annual CSP analysis the monitoring of SWIFT's fraud and detection tools, such as the Sanction Screening Service, which screens financial messages against international sanction lists before sending it through SWIFT's network, and the Payment Control Service, which filters a message against certain user-set rules before the message can be processed. SWIFT offers various tools to prevent and detect fraud incidents to help its users combat fraudulent payments and strengthen their existing security measures. Overseers include the effectiveness and enhancements of such SWIFT tools in their annual review. This is in line with the CPMI's strategy for reducing the risk of wholesale payments fraud related to endpoint security.

In 2020, overseers assessed the transparency and rigour of SWIFT's communication processes to its users in the event of technology changes, fraudulent compromises, and updates on common fraud practices in the industry. The CSP dedicates information-sharing as one of its foundational pillars supporting its users to adequately improve their incident and risk management processes. SWIFT's Information Sharing and Analysis Centre (ISAC) provides users with actionable business knowledge on cyber threats, indicators of compromise, and used hackers' techniques, tools and procedures. SWIFT targets both technical and business professionals through its ISAC portal facilitating a digestible format for information-sharing.

Cyber attacks targeting SWIFT participants have continued over the course of 2020, which are not expected to slow down. Overseers obtaining reasonable assurance on the effectiveness of the CSP and its features benefits the overall financial community in terms of reducing fraudulent transactions as a result of cyber hacks. The oversight objective remains to ensure that the security requirements evolve in line with new threats, improvements in cyber security capabilities and regulatory expectations.

COVID-19

Since the functioning of the financial sector heavily relies on SWIFT's core messaging services, overseers closely followed up on SWIFT's responsibility to ensure its operations as critical infrastructure during the materialised extreme scenario of a worldwide pandemic outbreak. Therefore in 2020, the COVID-19 impact on SWIFT, the company's response to it and implementation of mitigating actions became a standing topic under overseers' review activities. They conducted such analysis based on frequent written statements provided by SWIFT and multiple interactions with members of the Executive Management on SWIFT's security status and risk monitoring.

Like many other international organisations, SWIFT had to adapt and react to the impact of COVID-19. SWIFT began early monitoring of the situation in accordance with national and local authorities' measures. Given its role as critical service provider, SWIFT's main priority was to safeguard the operationality and availability of its critical messaging infrastructure avoiding any global interruption. Despite the closure of multiple offices, SWIFT has been able to ensure business continuity of its services thanks to generalised working from home for its employees, and the reorganisation of staff being able to work at the necessary SWIFT locations.

To lower the burden on its customers, SWIFT implemented several mitigating measures, which are further detailed in the box below.

BOX 12

Mitigating initiatives taken by SWIFT

In order to reduce the operational burden on its users in context of the pandemic and generalised working from home, SWIFT decided to implement multiple mitigating actions regarding the Customer Security Programme (CSP), and the yearly Standards Release. Before SWIFT had implemented the mitigations, overseers sought assurance in their analysis that these would not cause any drawbacks to the targeted CSP security objectives in the SWIFT user community.

SWIFT implemented the following CSP mitigations:

- For 2020, customers needed to re-attest against the existing set of CSCF v2019 controls by December 2020. The updated CSCF v2021 will come into effect in July 2021, with the normal year-end deadline for compliance. The CSCF v2021 includes a promoted advisory control to mandatory regarding the restriction of internet access in the IT infrastructure in the user environment that connects to the SWIFT network.
- The independent assessment for self-attestations (i.e. the requirement to get an opinion of the accuracy of the self-attestation from either an independent internal assessor or an external third-party assessor) will be aligned with the CSCF v2021.
- The next round of sampled mandatory external assessments will also be launched in line with the CSCF v2021.

A second mitigating action consisted of a scope reduction of the 2020 Standards Release. SWIFT decided to prioritise the standard changes for the securities messages. All initially planned other changes for 2020 have been postponed to November 2021. The 2021 Standards Release will include the 2020 changes (excluding the securities' standard changes) and agreed 2021 changes.

For 2021, overseers expect the adoption of the independent assurance framework and the resumption of mandated external audits and will review their outcomes.

Other topics

In addition to the overseers' considerable attention on CSP and the COVID-19 impact on SWIFT, the overall focal point remains on the security and availability of SWIFT's activities and core messaging services at any given time or circumstance.

Overseers' yearly activities are based around the five High-Level Expectations (HLEs).

For the first HLE "Risk Identification and Management", overseers assess SWIFT's Enterprise Risk Management (ERM) and audit activities. Included in this review are the effectiveness and independence of these lines of defence, and their interactions with each other. Overseers have revised the further maturing of SWIFT's risk management practices and how the second line of defence coped with the impact of the pandemic on SWIFT on the short and longer term. It was and still is important that SWIFT achieves the most critical project objectives, even during a crisis. The functioning and control work of SWIFT's auditors has been challenged by overseers with continuous analysis on their provided opinions and findings. Frequent interactions with SWIFT's Chief Risk Officer and Chief Auditor have given better insight into these above-mentioned topics.

Cyber security, which falls under the second HLE "Information Security", remains a major priority for overseers. Each year, there is a thorough analysis of SWIFT's proposed cyber security strategy and security roadmap activities. Overseers expect that SWIFT foresees the necessary investment and maintains the maturity of key security capabilities to safeguard the functioning of its critical messaging services. The evaluation of the design, implementation and improvement of cyber detection, response and recovery capabilities contributes to obtain such assurance. As a sequel to the first in-depth on-site review on ERM in 2018, a second on-site review took place virtually in 2020 on SWIFT's cyber security, which has not been finalised yet. A second large pillar of HLE 2 is the CSP, which is described in paragraph "Customer Security Programme" above.

Incidents and business continuity are vested in HLE 3 "Reliability and Resilience". Overseers investigate incidents that disrupt SWIFT's services. For each incident, SWIFT shares with the overseers the sequence of the incident events, impact on its users, and action plan to avoid similar incidents in the future. Overseers share their expectations to SWIFT on the incident management processes so that this critical communication continues to be refined. Considering the pandemic, the precautionary and responsive measures that SWIFT undertook to maintain business continuity have also been included in the oversight discussions.

For HLE 4 "Technology Planning", overseers closely follow up on the impact of new technologies and processes on the entire SWIFT organisation and its community. In 2020, SWIFT launched its new strategy in which there

will be a shift of the current sequential messaging to end-to-end transactions. This change will be aligned with the ISO 2002[2] migration of cross-border payments and cash management. In this approach, SWIFT envisages that users will be able adopt the ISO 20022 format at their own pace. SWIFT's new strategy reorientation was often put on the agenda in the course of 2020 to better grasp the alignment between its business and IT strategies, more specifically the project development steps, milestones and interaction with customers. This will be continued in 2021.

During 2020, overseers organised a deep dive on HLE 5 "Communication with Users". The objective for this session was to have a first dedicated interaction with SWIFT's recently appointed Chief Customer Experience Officer. The deep dive provided overseers with insight into the objectives of SWIFT's communication with customers and the processes to ensure care across all customer touchpoints. This will become ever more important for the further roll-out of SWIFT's new strategy course and ISO 20022 migration start in 2022. Overseers are keen on analysing the coming developments.

4.3 Oversight priorities in 2021

Overseers follow a risk-based approach for the yearly planning of SWIFT oversight activities. Each quarter, they evaluate the covered topics and use this information to identify which items or domains require additional critical review or which new topics need to be included in future analysis. Thanks to this method, overseers have the flexibility to add items or change the review frequency of certain topics, which contributes to the continuous oversight format throughout the entire year.

In 2021, the changing environment in which SWIFT operates and the company's anticipation of such changes will be on the agenda. More specifically, the focus remains on the adequacy of SWIFT's cyber management and strategy to cope with the ever-evolving cyber threat. Part of the analysis includes the review on SWIFT's cyber security roadmap and corresponding investment plan. Each year, overseers also challenge the provided ISAE 3000 reports of SWIFT's external security auditor.

Technological changes and their impact on SWIFT will also be one of the top oversight priorities in 2021. Overseers will continue to seek assurance that the corresponding risks in these domains are adequately assessed, managed, and mitigated for SWIFT to ensure business continuity of its services.

Another oversight top priority remains the different components of the CSP. A sub-set of certain follow-up CSP items include the following: CSCF control framework consultation process and its effectiveness, refinement of existing and additional CSP metrics, compliance levels of SWIFT's community against the mandatory and advisory security controls, further maturing of supervisory authorities' involvement, outreach to relevant stakeholders, outcomes of the mandatory independent assessments.

On top of these areas, a fourth major category covers standing topics, such as interactions with SWIFT's risk department, review of internal audit reports, follow-up of incidents and associated action plans, operational resilience activities and other.

The five HLEs lie at the heart of the overall oversight analysis work and planning. These HLEs form the starting point of identifying the topics to cover annually from a risk-based perspective. Since there is an extensive set of topics to be covered by overseers each year, the following items are a shortlisted indication of topics that will be included in 2021:

- HLE 1 Risk Identification and Management:
  - SWIFT's overall risk profile and topic-specific risk assessments;
  - internal and external audit findings, and identified mitigations that management undertakes.

- HLE 2 Information Security:
  - Customer Security Programme KYS functionality;
  - attack vectors of logical intrusion tests.
- HLE 3 Reliability and Resilience:
  - business continuity management enhancement;
  - impact of technological evolutions on SWIFT's resilience.
- HLE 4 Technology Planning:
  - changes in technology risk on existing IT infrastructure;
  - platform that facilitates ISO 20022 transactions.
- HLE 5 Communication with Users:
  - SWIFT's communication on ISO 20022 migration towards customers;
  - customer experience roadmap.