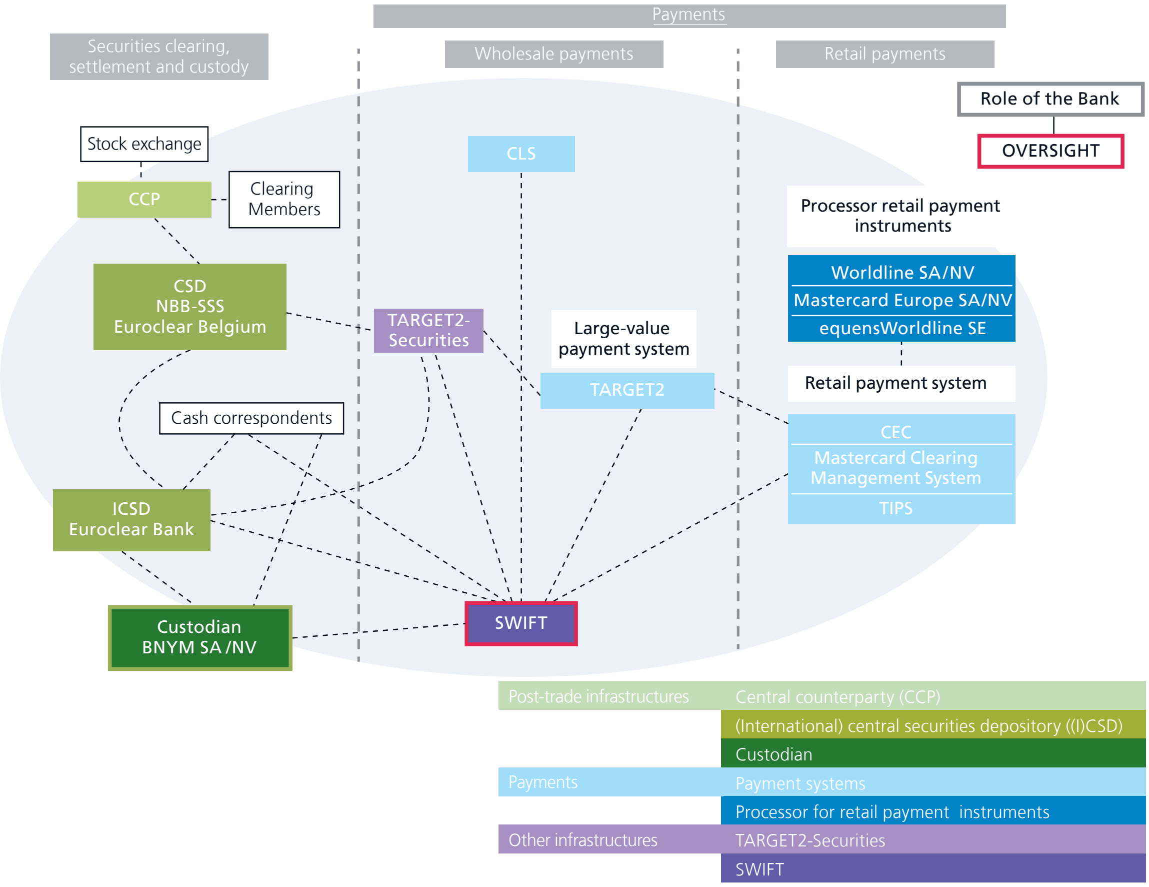
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company that provides messaging services to financial institutions and market infrastructures across the globe. SWIFT serves different customer types which vary in terms of size and activity: banks, brokers, investment managers, fund administrators, custodians, corporates, and treasury counterparties. SWIFT is registered in Belgium with its headquarters located in La Hulpe.

Through its financial messaging services, SWIFT fulfils a crucial role in facilitating correspondent banking and financial market infrastructure activities. Such a fundamental role for the global financial industry creates significant systemic dependency on SWIFT. Hence, the G10 jurisdictions established the cooperative SWIFT oversight framework to monitor SWIFT's activities with the aim of safeguarding financial stability.

Chart 4

SWIFT as a critical service provider to the financial industry



4.1 SWIFT oversight framework

4.1.1 SWIFT and its users

National member groups are represented by SWIFT's users and are organised per jurisdiction. These users own and control the company and are involved in the appointment of SWIFT Board members. SWIFT's share distribution is based on the message traffic, ensuring that the Board represents the jurisdictions with the largest users, i.e. with the highest message traffic volumes. Since message traffic proportionality is not static, the shares are reallocated every three years to mirror the actual SWIFT user community. In 2021, such a redistribution took place but did not result in the introduction of any new jurisdictions on the SWIFT Board. The next share reallocation is scheduled for 2024.

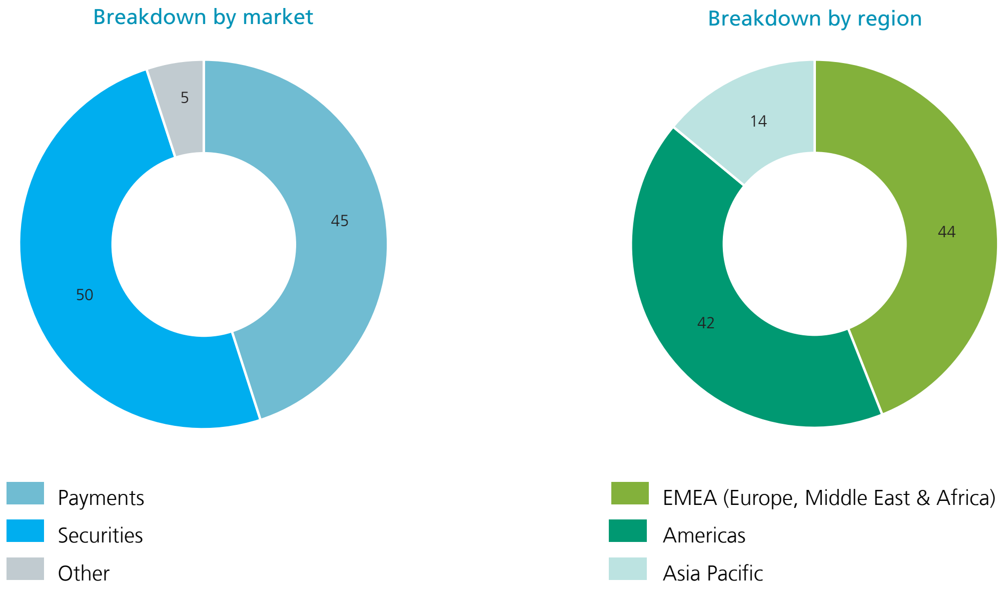
SWIFT provides messaging services to customers from more than 200 countries, amounting to approximately 11000 SWIFT users. The following numbers reflect SWIFT's global presence: in 2021 10.6 billion messages were sent with a daily average of 42.0 million messages. Despite the continued Covid-19 pandemic, SWIFT achieved double-digit growth of 11 % in 2021 compared to 2020. The main contributors to this growth were the economic recovery and the securities market volatility, sparked by higher volumes of securities settlement instructions.

The core messaging service for exchanging financial messages is SWIFT's FIN application. The following figure depicts SWIFT's FIN traffic for 2021 distributed per region and market. There was a total of 11642 live users, of whom 2421 are SWIFT's shareholders belonging to different national member groups. In line with figures for previous years, the payments (45.3 %) and securities (49.7 %) markets represented the lion's share of SWIFT's messaging for 2021. The Europe, Middle East and Africa (EMEA) region claimed the largest part of the total 2021 FIN traffic volume, closely followed by the Americas and UK region.

Important to note is that, for the ISO 20022 migration for cross-border payments and cash management, use of the FIN messaging service will gradually give way to the FIN Plus service (or InterAct service). The FIN end-of-life for this type of messages will coincide with the planned end of the ISO 20022 migration in 2025.

Chart 5

SWIFT FIN traffic distribution by region and market



Source: SWIFT.

4.1.2 International cooperative arrangement

In 1997, the G10 central banks formalised the SWIFT oversight arrangement for the purpose of monitoring the adequate and safe functioning of the critical service provider. In addition to the participating G10 jurisdictions, the Bank for International Settlements and the European Central Bank are represented in the international working groups. As SWIFT is headquartered in Belgium, the NBB is the standing lead overseer and chairs the international oversight meetings.

The G10 central banks are represented in the four working groups: *the Technical Group* (TG) which conducts technical fieldwork, the *Cooperative Oversight Group* (OG) which is the decision-making body and sets the oversight strategy, the *Executive Group* (EG) which serves as the interface for overseers to communicate conclusions and recommendations to SWIFT's Board and Executive Management, and the *SWIFT Oversight Forum* (SOF) which involves a wider group of central banks discussing the oversight activities and relevant changes at SWIFT.

Given the systemic character of SWIFT, a wider group of G20 jurisdictions are also directly involved in the oversight. These G20 central banks are represented in the SOF working group. Their membership corresponds to their share in the total SWIFT traffic volume and the CPMI membership composition. The SOF deals with the SWIFT oversight conclusions, planning and priorities, Customer Security Programme and discussions on dedicated topics.

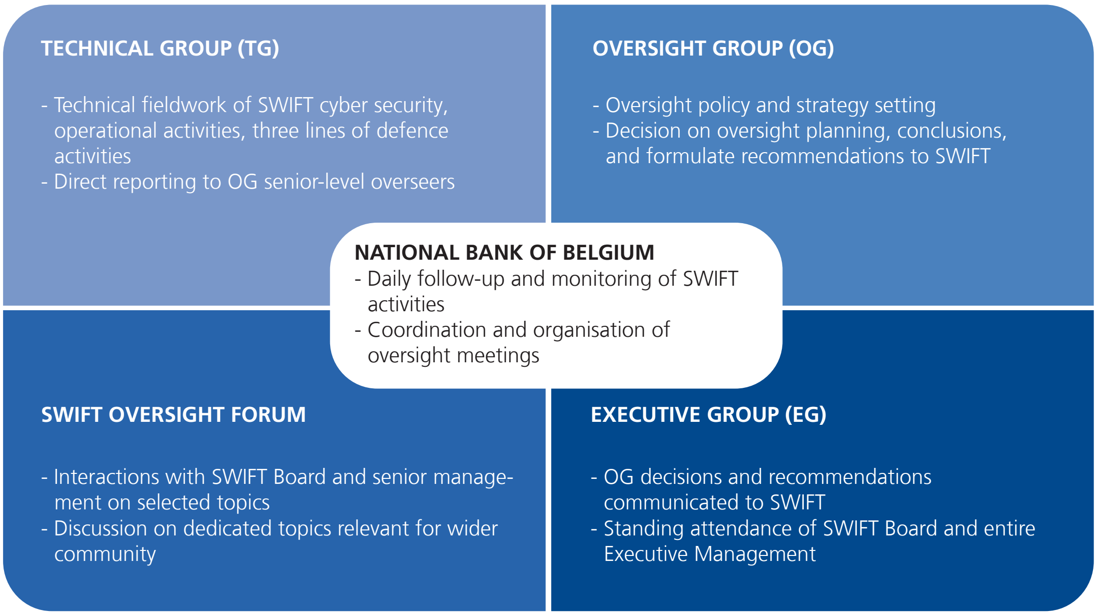
In its capacity as SWIFT's lead overseer, the NBB has a dedicated team which conducts daily monitoring and follow-up of SWIFT's activities and projects. As formulated in the SWIFT Oversight Protocol, the NBB serves as the entry point for channelling information to the other overseers and, as chair, coordinates the different working groups in terms of reporting to the other overseers and preparing discussion items for them.

More detail on the composition and scope of activities for each of the working groups can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

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

Figure

SWIFT oversight working groups involving G10 and G20 central banks



TECHNICAL GROUP (TG)

- Technical fieldwork of SWIFT cyber security, operational activities, three lines of defence activities
- Direct reporting to OG senior-level overseers

OVERSIGHT GROUP (OG)

- Oversight policy and strategy setting
- Decision on oversight planning, conclusions, and formulate recommendations to SWIFT

NATIONAL BANK OF BELGIUM

- Daily follow-up and monitoring of SWIFT activities
- Coordination and organisation of oversight meetings

SWIFT OVERSIGHT FORUM

- Interactions with SWIFT Board and senior management on selected topics
- Discussion on dedicated topics relevant for wider community

EXECUTIVE GROUP (EG)

- OG decisions and recommendations communicated to SWIFT
- Standing attendance of SWIFT Board and entire Executive Management

BOX 7

COVID-19 and SWIFT oversight

With the sudden outbreak of the Covid-19 pandemic in 2020, overseers had to make alternative arrangements for their activities to ensure the adequate oversight of SWIFT. Given the travel restrictions imposed by different jurisdictions, the only possibility was to set up virtual meetings.

Previously, TG members traditionally reviewed the majority of topics at set times in physical meetings with SWIFT's three lines of defence. In order to cover all necessary topics on the agenda for the year and assess the impact of the pandemic on SWIFT, the topics for review were scheduled over 2 six-month periods so that the TG could submit its crucial reports to the OG members at the two OG meetings in the year. In line with the TG's decentralised way of working, the other senior level working groups (i.e. OG, EG, SOF) were also held in virtual form. In 2020, overseers successfully executed all activities as initially scheduled in the planning for that year despite the decentralised working approach. The three guiding principles (i.e. (i) focus on operational risks, (ii) review critical business, technology and IT projects, and (iii) obtain assurance on the effectiveness of the three lines of defence) which were defined in 2020 to refocus the TG activities also served as guidance for the 2021 planning.

The same decentralised approach was applied to the 2021 oversight of SWIFT. The TG activities were spread over the first and second half of the year. The TG's conclusions and recommendations were reported to the OG according to the standard procedure specified in the oversight arrangement. The OG and EG working groups were also able to cover the required topics for discussion. A SOF meeting to report on the 2021 activities and 2022 priorities was held in January 2022. Overall, the outlined 2021 priorities were not affected by the Covid-19 pandemic, and overseers continued their critical review on SWIFT's activities with a strong focus on cybersecurity and operational risk.

On-site reviews (OSRs) are a recent addition to the SWIFT oversight toolbox and their purpose is to obtain deeper knowledge on certain subjects at SWIFT. After offline documentation analysis by the OSR team, the overseers organise dedicated physical interactions with SWIFT representatives to obtain a full view of the aspects concerned. Due to the travel restrictions caused by the pandemic, the second OSR on cybersecurity was conducted virtually. Nevertheless, overseers were able to interact virtually with SWIFT and successfully completed their review, resulting in conclusions and recommendations. For the third OSR which will start in 2022, in-person meetings are preferred, but with the current pandemic situation this will most likely not be possible. Either way, overseers will be able to execute the planned OSR and, if possible, switch between virtual and in-person meetings if circumstances permit.

The common thread of SWIFT oversight is based on 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. These five HLEs are included as Annex F to the CPMI-IOSCO Principles for FMIs and are the generic oversight requirements for all critical service providers to FMIs.

The overseers' review activities are all rooted in the five HLEs and drive the oversight planning and priorities. Overseers assess the adequacy of SWIFT's management of operational and security risks over all three lines of defence by comparing it with these expectations. SWIFT is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. documentation, interactions with SWIFT's three lines of defence, and discussions with Executive Management and Board).

More detail on the specific description of the five HLEs can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

4.2 Selection of major topics reviewed by overseers in 2021

This paragraph covers a non-exhaustive selection of major topics which overseers analysed in 2021. The highlighted topics are a subset and are not a full representation of the review work conducted in 2021 (e.g. standing topics such as business continuity exercises, effectiveness of three lines of defence, enterprise risk management, and internal audit activities).

4.2.1 Impact of covid-19 on SWIFT

The core messaging services facilitated by SWIFT are of systemic importance for the global financial industry. Therefore, overseers closely monitored to what extent the pandemic affected SWIFT, and the mitigating actions taken by SWIFT to address and prepare for certain developments. The main focus of the overseers' assessment was the impact on SWIFT's projects, security, and resilience. SWIFT shared frequent statement updates with overseers on certain changes to measures taken, and SWIFT's Chief Risk Officer (CRO) provided a status update on the Covid-19 situation for SWIFT.

As in 2020, SWIFT was able to ensure the business continuity of its operations and core messaging services. SWIFT's approach to the pandemic in 2020 proved effective and was also applied to the 2021 activities (i.e. working from home, health protection measures, and shifts for critical staff on-site). Given its global presence, SWIFT adhered closely to local laws and rules in order to take appropriate action. Some jurisdictions eased or tightened certain restrictions, so that SWIFT also had to adjust its measures in some locations (e.g. reopening of offices).

Overseers concluded that the mitigating actions taken by SWIFT were adequate to address the Covid-19 pandemic throughout 2021, ensuring the continuity of its business operations and avoiding any global interruption affecting the financial community. The monitoring on this subject will continue in 2022.

4.2.2 Messaging traffic

In 2020, there was some decline in payments traffic via SWIFT's network because of the numerous lockdowns imposed by governments to contain the Covid-19 pandemic, causing global economic activity to slow down and businesses to close. In 2020, SWIFT's payments traffic grew by 2.4 % compared to 2019, which was below the growth trend of the previous years. Thanks to the economic uncertainty and market volatility, SWIFT achieved double-digit growth of 18.3 % in its securities traffic. Overall FIN activity recorded 10.3 % growth in 2020.

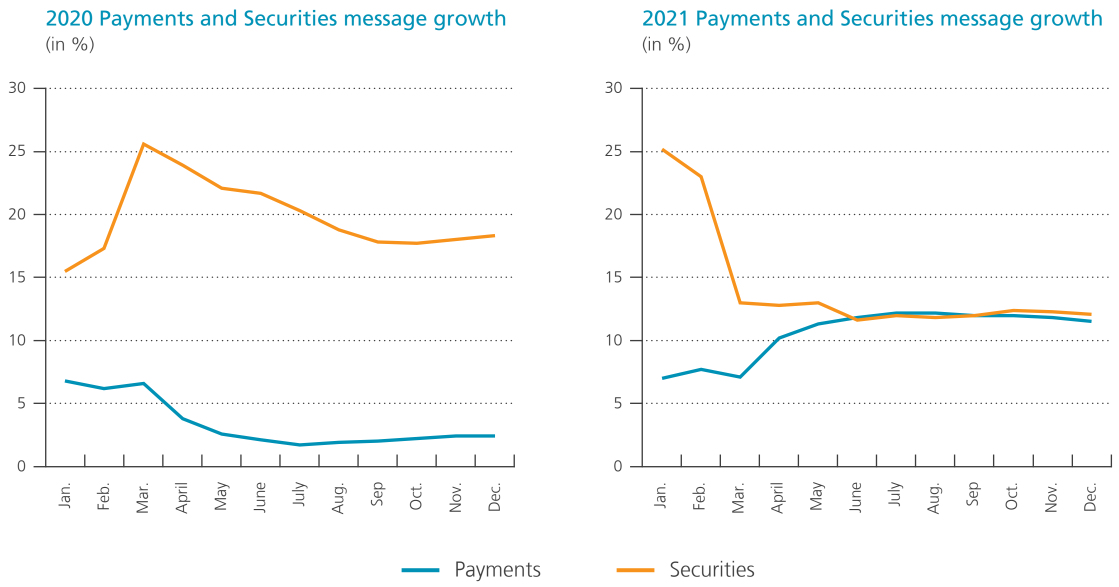
Given the continued uncertain economic climate, SWIFT expected its FIN messaging traffic to grow by a modest 4.2 % in 2021. However, there was a double-digit increase in both payments (11.5 %) and securities traffic (12.1 %). Thanks to the gradual economic recovery and permanently high volumes of securities settlement instructions, SWIFT recorded FIN traffic growth of 11.4 % for 2021, well above the budgeted figure.

Overseers conduct an annual review of SWIFT's messaging traffic. That analysis helps to provide a comprehensive view of the extent of the community's dependence on SWIFT's messaging services. In addition, the fluctuations in message traffic reflected certain trends triggered by the pandemic (e.g. less payments traffic and more securities traffic as a result of lockdowns and economic uncertainty). Overseers conclude that, despite an extreme event such as a pandemic, SWIFT remains highly important for the global financial sector, and that underlines the pertinence of appropriate oversight on SWIFT.

The following two graphs show the changes in payments and securities traffic in 2020 and 2021. At the beginning of the pandemic in early 2020, the growth of payments message traffic decreased, while a peak can be observed for the securities market. This could be explained by the economic uncertainty causing higher volatility on financial markets. For 2021, the growth of payments and securities traffic converged, with both markets recording stable growth in double digits as of April. The more favourable economic outlook could be the main factor here.

Chart 6

Growth of Payments and Securities message traffic in 2020 and 2021



Source: SWIFT.

4.2.3 Customer Security Programme

The Customer Security Programme (CSP) has been high on the overseers' agenda ever since the programme started after the 2016 Bangladesh case. SWIFT has built up an extensive programme enhancing the cybersecurity of its users, their counterparts, and the entire community. Through the CSP, users are required to adhere to certain controls and good practices to appropriately secure their on-premises IT environments connecting to the SWIFT network. With cyber-attacks continuing in the financial sector, overseers seek reasonable assurance on the effectiveness of the CSP and corresponding initiatives, designed to adapt to new threats, improve cybersecurity capabilities, and adhere to regulatory expectations.

Over the years, SWIFT has taken multiple initiatives and improved various aspects of the CSP, such as the yearly review of the Customer Security Control Framework (CSCF), improvements to the Know-Your-Customer (KYC) tool, launch of an independent assessment framework, introduction of mandated assessments, more effective involvement of supervisors, actionable updates on the Information Sharing and Analysis Centre (ISAC) portal, and organisation of recurring awareness campaigns. Thanks to these actions, SWIFT reported to overseers that there has been a downward trend in customer cases. Overseers have followed up on this and, despite the CSP's successful record, SWIFT is expected to continue to enhance the programme.

One such expectation concerns the involvement of supervisory authorities in using the CSCF self-attestation data of financial institutions. From the beginning, overseers have encouraged SWIFT's move to engage supervisors more directly in making effective use of the rich self-attestation data of its users, which could provide crucial input for supervisors' risk-based planning and scoping. The identification and onboarding of the relevant supervisory authorities in the Know-Your-Supervisor (KYS) tool have proven to be challenging because some jurisdictions have multiple supervisory authorities relevant for one country. According to SWIFT's first reporting to overseers, the use of the self-attestation data by the onboarded supervisory authorities for financial institutions within their relevant jurisdictions has fallen short of expectations. Overseers have stressed the importance of this entire initiative and will continue to monitor the actions required to improve the supervisory onboarding and safeguard the effectiveness of the KYS application.

As per standard procedure, overseers contributed, together with the national member groups, to the yearly review of the Customer Security Control Framework (CSCFv2022), which resulted in control clarifications, and the change of two controls encouraged by overseers :

i. Promotion of the "advisory" control "*2.9 Transaction Business Controls*" to "mandatory", helping to achieve the CPMI endpoint strategy for reducing the risk of wholesale payments fraud. Control 2.9 has the control objective to "*ensure the outbound transaction activity within the expected bounds of normal business hours*".

ii. Introduction of the new advisory control "*1.5 Customer Environment Protection*" which has the control objective to "*ensure the protection of the customer's connectivity infrastructure from external environment and potentially compromised elements of the general IT environment*".

SWIFT users are expected to be compliant with the mandatory security controls (i.e. security baseline) and can also attest their compliance with the advisory controls (i.e. good practices for securing local IT infrastructures). A user's self-attestation (i.e. compliance with the CSCF security controls) is uploaded to the Know-Your-Customer Self-Attestation (KYC-SA) tool by the end of each year. The new CSCF version (v2022) was introduced in mid-2021, and users have until the end of 2022 to submit their attestations.

By 31 December 2021, 86 % of SWIFT customers had provided a valid attestation in respect of the CSCF controls, and of these self-attestations 78 % indicated compliance with the mandatory controls. The compliance levels and the number of self-attestations are in line with the uptake in 2019 and 2020. Through SWIFT's quality assurance and monthly metrics reports, overseers closely monitor various CSP-related metrics, such as the users' attestation and consultation levels. The reporting on CSP metrics is crucial for overseers to obtain a view of the cybersecurity stance of the SWIFT user community. As such, overseers expect SWIFT to refine and extend the CSP reporting metrics as appropriate.

The launch of the mandated independent assessments in addition to the self-assessments had been delayed by one year because of the Covid-19 pandemic. As a mitigating measure to ease the operational burden on its community, SWIFT postponed the launch to 2021. In the meantime, the so-called Independent Assessment Framework (IAF) was launched in mid-2021. Overseers await the results of the IAF to analyse the effectiveness of the initiative and will request additional information, if necessary.

Overseers also assess SWIFT's processes for communication with its users regarding the use of new technologies, fraud cases, and common cybersecurity threats affecting the community. SWIFT's Information Sharing and Analysis Centre (ISAC) provides its users with actionable information on cyber threats, indicators of compromise and common hacking practices. For example, through the ISAC portal SWIFT shared relevant information on the Log4j vulnerability and the actions SWIFT users should undertake. The timeliness and comprehensiveness of the information sharing on such events is also covered by the overseers' review.

4.2.4 ISO 20022 migration

SWIFT has announced that it will migrate the cross-border payments and cash reporting messages from the FIN MT standard to the richer ISO 20022 MX standard, at the request of the community. The richer and standardised information is intended to promote greater transparency and speed, and lower cost for cross-border payment transactions. SWIFT originally planned to initiate the migration phase in November 2021 but has moved the launch date to November 2022. The overall co-existence period during which users will be expected to switch from FIN MT to ISO 20022 MX will start in 2022 and end in November 2025. This timeline extension was driven by industry feedback to ensure that the community can adopt the ISO standard at their own pace and to limit the corresponding investment costs necessary to achieve the intended benefits.

As a global standard setter, SWIFT takes the lead in coordinating the ISO 20022 migration for its community. From the beginning, overseers have closely monitored SWIFT's approach, project management and planning, risk assessment, and communication with users. A recent development that SWIFT announced was the launch of the in-flow translation service, which will be made available for testing before the migration starts, and allows for the receipt of both FIN MT and ISO 20022 MX messages. With this service, SWIFT wants to ensure that participants can switch at their own pace during the co-existence period until November 2025. Overseers have closely analysed the scope and testing of the service. Overall, SWIFT announced that the migration preparations were progressing as planned up to the set deadline of November 2022.

BOX 8

G20 roadmap for enhancing cross-border payments

In 2020, the G20 agreed to make enhancing cross-border payments a priority, with the aim of promoting faster, cheaper, more transparent, and more inclusive cross-border payment services, including remittances, while maintaining their safety and security. This would have widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion.

The Financial Stability Board (FSB), in coordination with the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and other relevant international organisations and standard-setting bodies, developed a roadmap to address the key challenges faced by cross-border payments. This roadmap sets out specific actions and indicative timelines. It encompasses 19 building blocks, one of which, namely building block 14, focuses on ISO 20022. The purpose of this building block 14 is to adopt a harmonised ISO 20022 version for message formats. The following key milestones, as described in the Stage 3 Roadmap Report[1], have been defined to achieve the overall objective of building block 14:

- CPMI and BIS Innovation Hub host a TechSprint on ISO 20022 for cross-border payments.
  Hackathon has been successfully completed;
- CPMI assesses suitability of existing ISO formats for cross-border payments and facilitates the development of market guidance in collaboration with relevant stakeholders, including the High Value Payments Plus (HVPS+) market practice task force and the Cross-Border Payments and Reporting Plus (CBPR+) working group.
  Work in progress;

[1] For more detailed information, see https://www.bis.org/cpmi/publ/d193.htm and https://www.fsb.org/wp-content/uploads/P131020-1.pdf

- CPMI members and national authorities publish plans for adopting a harmonised version of ISO 20022. *Work in progress;*
- CPMI, in cooperation with public/private sectors, develops an implementation guide on ISO 20022, including conversion/mapping.
  Work in progress.

To achieve the goals of building block 14, the CPMI is cooperating with the Payment Market Practice Group[1] (PMPG) to develop market guidance on ISO 20022 for cross-border payments. The PMPG is a global industry forum composed of bank representatives from communities in the global payments market. The PMPG's mission is "*to drive better market practices which, together with correct use of standards, will help in achieving full STP [straight-through processing] and improved customer service*". The PMPG oversees the development of various standardisation initiatives, including HVPS+ (High-Value Payment Systems Plus) and CBPR+ (Cross-border Payments and Reporting Plus) ISO 20022 message implementation guidelines. In this capacity, the PMPG is also involved in the ISO 20022 migration of cross-border payments and cash reporting messages. For the CPMI working group on building block 14, it is important to interact with the PMPG and build on existing work. Given the global reach of SWIFT's user community, SWIFT's work on ISO 20022 has been a relevant source of information for the working group and also for other building blocks (e.g. building block 15 focusing on the harmonisation of API protocols for data exchange).

[1] For more information, see https://www.swift.com/about-us/community/swift-advisory-groups/payments-market-practice-group

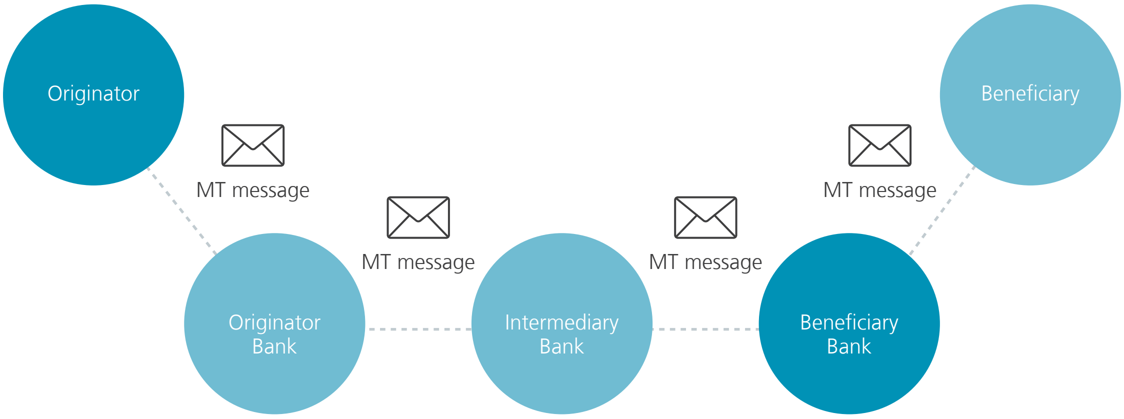
4.2.5 Transaction Management Platform

In 2019, SWIFT revealed their plans to build the Transaction Management Platform (TMP), moving away from traditional sequential messaging to end-to-end transactions. The planned launch of the platform coincides with the start of the ISO 20022 migration co-existence phase in November 2022. However, the move from FIN MT to ISO 20022 MX is not dependent on the activation of the TMP, and the two projects are totally separate.

As the following figure illustrates, SWIFT's current message flow consists of MT messages forwarded from originator to beneficiary using SWIFT's secure communications channel. SWIFT's processing is message-driven and there is no central notion of the end-to-end transaction generating the underlying messages between all parties involved.

Figure

Current sequential SWIFT message flow

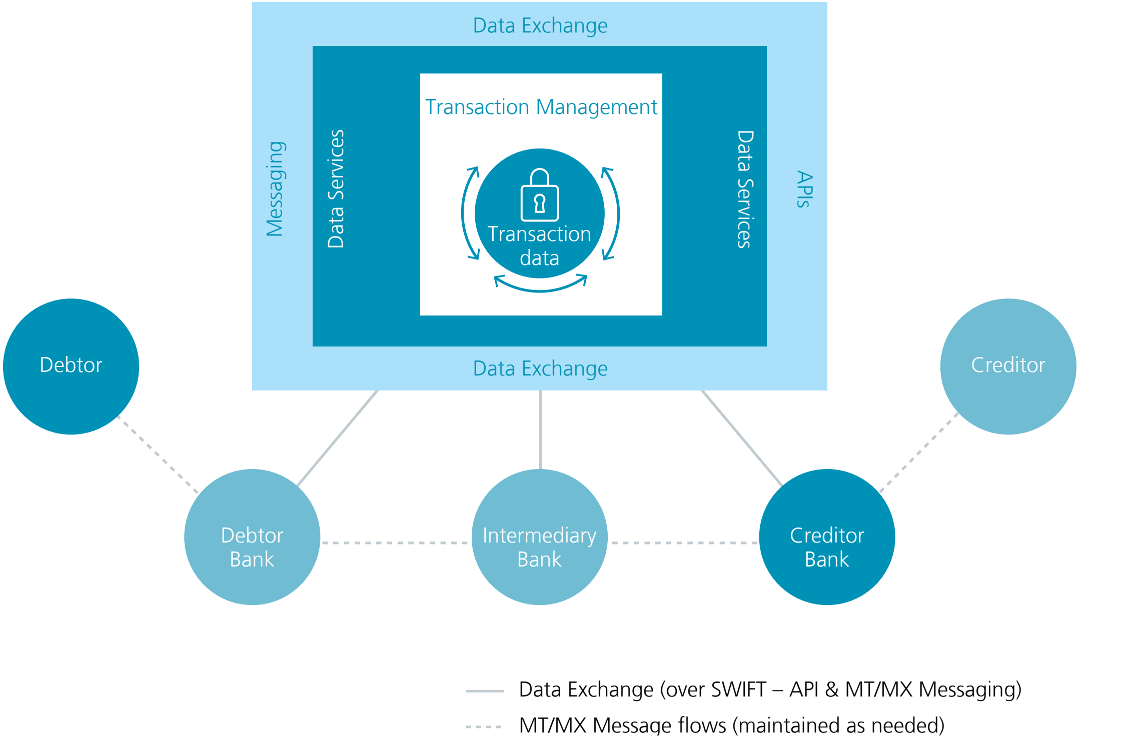


Source : SWIFT.

By evolving from secure message forwarding to end-to-end transaction management orchestrated by TMP, SWIFT wants to use richer data and reduce friction (i.e. provide better customer experience, increased efficiency, and new value-added services such as transaction validation). The following figure shows that the underlying communication channel for a transaction is format agnostic and could be FIN MT, ISO 20022 MX or Application

Figure

Planned end-to-end SWIFT transaction flow



Source : SWIFT.

Programming Interfaces (APIs), or a combination of channels based on the capabilities of the transaction parties involved (i.e. backward compatibility). The platform maintains full transaction data accessible to any authorised party in the transaction chain, helping to ensure end-to-end transparency. TMP also facilitates the use of APIs so that authorised users can retrieve the transaction status via an API call over the SWIFT network.

TMP has a major impact on SWIFT's core messaging operations since it changes the payment message flow approach. Therefore, overseers have repeatedly conducted thorough reviews to obtain a complete picture of all relevant HLE aspects of TMP: analysis of risk assessments and corresponding mitigating actions, security and resilience features of the platform, architectural blueprint, project management, customer communication and engagement initiatives. Since TMP touches upon all five HLEs, the project has been part of the continuous oversight monitoring activities. Despite SWIFT confirming project delivery within the planned timeframes by November 2022, overseers will continue their critical and risk-based review of the project throughout 2022 and after its launch.

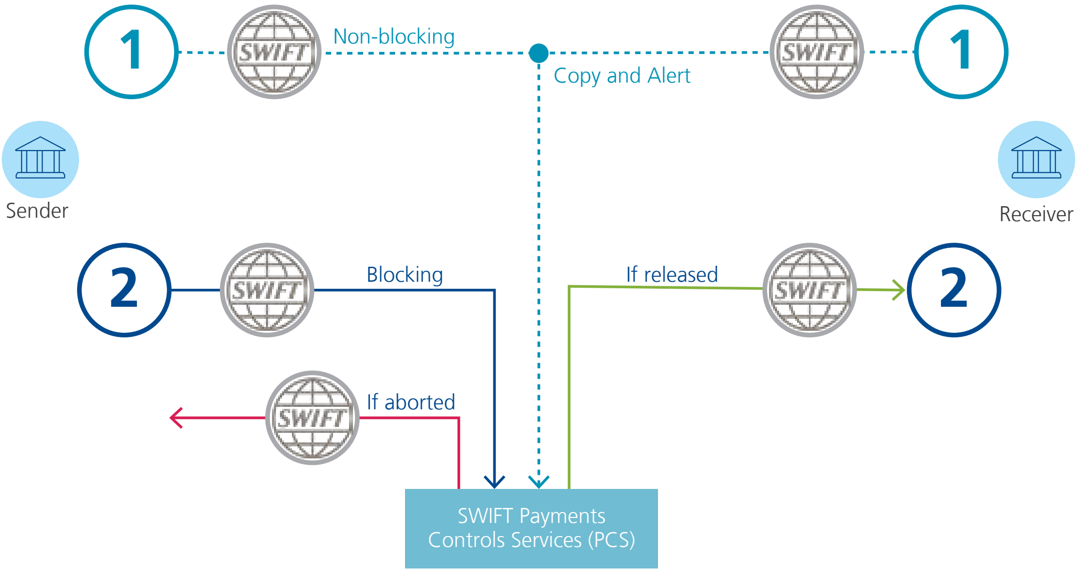
4.2.6 Financial Crime Compliance

SWIFT's Financial Crime Compliance (FCC) portfolio contains a broad set of services with the aim of combating financial crime and payments fraud. The changing threat landscape obliges SWIFT to enhance its FCC tools and introduce new services that ensure a legitimate financial transaction. In 2021, overseers conducted a review of the changes made to SWIFT's existing FCC services. The inclusion of the FCC portfolio in the oversight activities aligns with the CPMI's strategy for reducing the risk of wholesale payments fraud related to endpoint security.

In 2018, SWIFT launched the Payment Controls Service (PCS) which is a rule-based fraud detection service, currently offered at the financial institution level. PCS provides real-time protection against pre-defined payment fraud patterns, and such early fraud alerting enables quicker recovery actions. Since its launch, the modus operandi of payment fraudsters has been continuously evolving. In order to take advantage of the anomaly capabilities of the PCS, SWIFT has developed more granular detection at account level. Encouraged by the community, SWIFT will use pseudonymised statistics from past transactions sent by the entire community over the SWIFT network. Such data would use the PCS anomaly capabilities, and eventually result in fewer false positives and reduced friction for customers in investigating alerts.

Figure

SWIFT Payment Controls Service flows

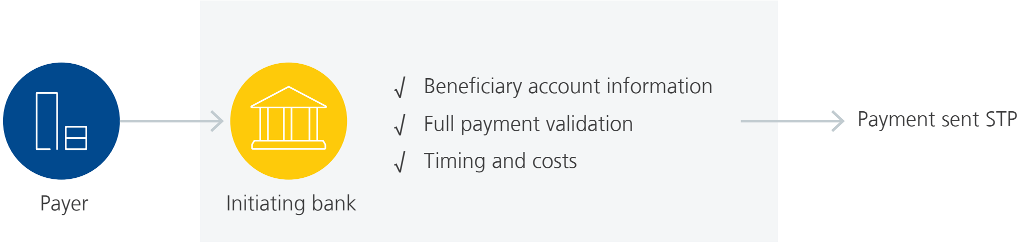


Source: SWIFT.

A similar approach will be applied to the Payment Pre-validation service activated in July 2021, which enables banks to check the beneficiary account information with the ultimate receiving banks in real time, and to verify if the data in the payment instruction is correct (i.e. destination country requirements). By using past transaction data, SWIFT wants to improve the speed and transparency of the service (i.e. central beneficiary account verification assesses the account validity based on pseudonymised account statistics).

Figure

SWIFT Payment Pre-validation service flow



Source: SWIFT

SWIFT plays a key role as a critical service provider with access to a large dataset. However, overseers will step up their monitoring of the corresponding risk assessment, the appropriateness of additional controls and measures to secure the extracted confidential data, and the technical implementation of the data storage infrastructure.

Overseers have also reviewed the changes to the Relationship Management Application (RMA), which manages financial institutions' business relationships. In order to accommodate the ISO 20022 transactions, SWIFT is converting the FIN MT-based service into a business-oriented model agnostic to the message formats used. To avoid misaligned relationships which are currently updated and stored in a decentralised manner, SWIFT will move the relationship data management to a central portal ensuring all users have access to the most up-to-date RMA relationships. The announced changes to the RMA have been analysed by the overseers, focusing on the technical set-up of the central repository, new business model and risk assessment.

4.2.7 Faster payment initiatives

Since its launch in 2017, SWIFT gpi has been repeatedly reviewed by overseers on its functionality, interaction with core messaging services, security aspects, enhancements, and adoption rates. In 2021, more than 4000 financial institutions were using the service, which represents 89 % of the cross-border payments sent over the SWIFT network and covers more than 200 countries.

In July 2021, SWIFT released the new SWIFT Go service, which is an interbank service that makes it quicker and cheaper for participating banks to send low value cross-border payments, with the possibility of instant settlement. SWIFT wants to ensure that the traditional bank sector remains competitive in the high-growth market of low-value cross-border payments. For SWIFT, SWIFT Go is a key building block to enable instant and frictionless cross-border transactions in the retail payments sphere. Conversely, SWIFT gpi facilitates high-value or wholesale cross-border payments.

The service currently handles rather limited traffic for a small number of customers, but both traffic and customer numbers are expected to increase gradually. For overseers, it is important to have a full understanding of the scope of the service, and monitoring will be stepped up as the service develops. SWIFT's faster payment initiatives have attracted overseers' attention for further monitoring.

4.2.8 Interface hardening

SWIFT offers its customers a range of connectivity packs and interface products which provide communication and messaging services for exchanging financial messages over the secure SWIFT network. Customers also have the option of connecting to the SWIFT network via a certified third-party service bureau. Such service bureaux adhere to SWIFT's Shared Infrastructure Programme, which requires the vendors to comply with both mandatory and advisory CSCF controls. A customer could opt for a service bureau interface as a lightweight solution, to decrease the on-premises SWIFT stack.

Driven mainly by the continuing cybersecurity threat, SWIFT executes a yearly interface hardening to better protect the user's local SWIFT environment. Overseers have analysed the release roadmap and the updated interface version including the new security features, and examined how SWIFT ensures successful adoption.

4.3 Focal points for oversight in 2022

The annual planning of SWIFT oversight is driven by a risk-based approach. The oversight risk assessment helps to maximise the effectiveness and efficiency of the review activities. The assessment of the 2021 activities feeds into the 2022 planning. After each quarter, overseers evaluate the topics analysed and decide which ones require deeper review, or the items for which SWIFT needs to provide additional information. This approach creates sufficient flexibility for overseers to dedicate more time to certain topics when needed, or to hold a follow-up discussion at a later stage.

SWIFT operates in a changing environment with continued increasing competition and rapidly evolving technologies. That context affects SWIFT's go-to-market strategy (e.g. agile software development) and operations (e.g. incident management), and poses additional challenges, such as the global scarcity of skilled resources and the changing cyber threat landscape. Overseers are aware of the pace of change and will continue to monitor how it affects SWIFT in terms of technology planning, resilience guarantees, risk assessments, security decisions and design choices, while keeping users properly informed. At all times, overseers seek assurance that the identified risks arising from new technology choices and major projects are adequately managed and mitigated, to ensure business continuity with comparable or better resilience.

The cybersecurity strategy and management also remain high on the overseers' agenda for 2022. Overseers analyse which security investments and enhanced capabilities will contribute to SWIFT's protection against the more sophisticated cyberattacks. The cybersecurity review also involves challenging the ISAE3000 reports conducted by SWIFT's external security auditor. These reports provide independent assurance on SWIFT's internal control policies, procedures and controls structured around the five HLEs. The ISAE3000 reports consist of rich information important to the oversight on SWIFT and are thoroughly reviewed each year.

The follow-up on CSP is also part of the oversight activities for 2022. Overseers will take a closer look at the supervisory involvement and the improvement measures that SWIFT will take, the CSCF review, the outcome of the first independent assessments, CSP metrics and further refinements, the SWIFT user community's level of compliance with the CSCF controls, developments concerning customer cases, results of the new cycle of mandatory independent assessments, and other relevant CSP initiatives and campaigns.

In 2022, overseers will also aim at further refinement of incident reporting to overseers, to obtain more timely and comprehensive information on incidents. With a more advanced cyber threat landscape, it is utterly paramount that overseers are kept abreast of incidents potentially impacting SWIFT and the wider user community.

Two large projects – TMP and ISO 20022 migration – will reach their delivery deadline in 2022. Overseers have already conducted recurring and thorough reviews of these two projects but will continue to do so during 2022, with a stronger focus on the final preparations before launch and communication with customers.

Another area covers major standing topics such as interactions with the risk department and internal audit. Each review cycle includes a dedicated touchpoint with the second and third lines of defence to gain a clear understanding of their activities and obtain their views on certain projects and developments at SWIFT. Following the on-site reviews (OSRs) of the second line of defence (2018) and of the first line of defence (2020), overseers decided to conduct such a review on the third line of defence in 2022. A dedicated OSR team of overseers has been identified and tasked with scoping the internal audit domains for analysis. Depending on the pandemic situation, the 2022 OSR will be organised virtually, in much the same way as the 2020 review on cybersecurity.

The oversight planning for the following year is structured around the five HLEs which form the starting point for selecting topics for review. Following a risk-based approach, the previous year's assessment forms the basis for the review activities of the coming year. For 2022 this resulted in an extensive set of topics to be analysed by overseers, of which the following are a subset:

- HLE 1 Risk Identification and Management
    - Operational impact of the pandemic;
    - Internal and external audit findings;
- HLE 2 Information Security
    - Cybersecurity roadmap
    - Customer incidents and forensic capabilities
- HLE 3 Reliability and Resilience
    - Business continuity exercises;
    - Impact of technological developments on SWIFT's resilience;
- HLE 4 Technology Planning
    - Financial Crime Compliance portfolio;
    - Transaction Management Platform & ISO 20022 migration;
- HLE 5 Communication with Users
    - Customer communication related to ISO 20022 migration;
    - Customer adoption plans.