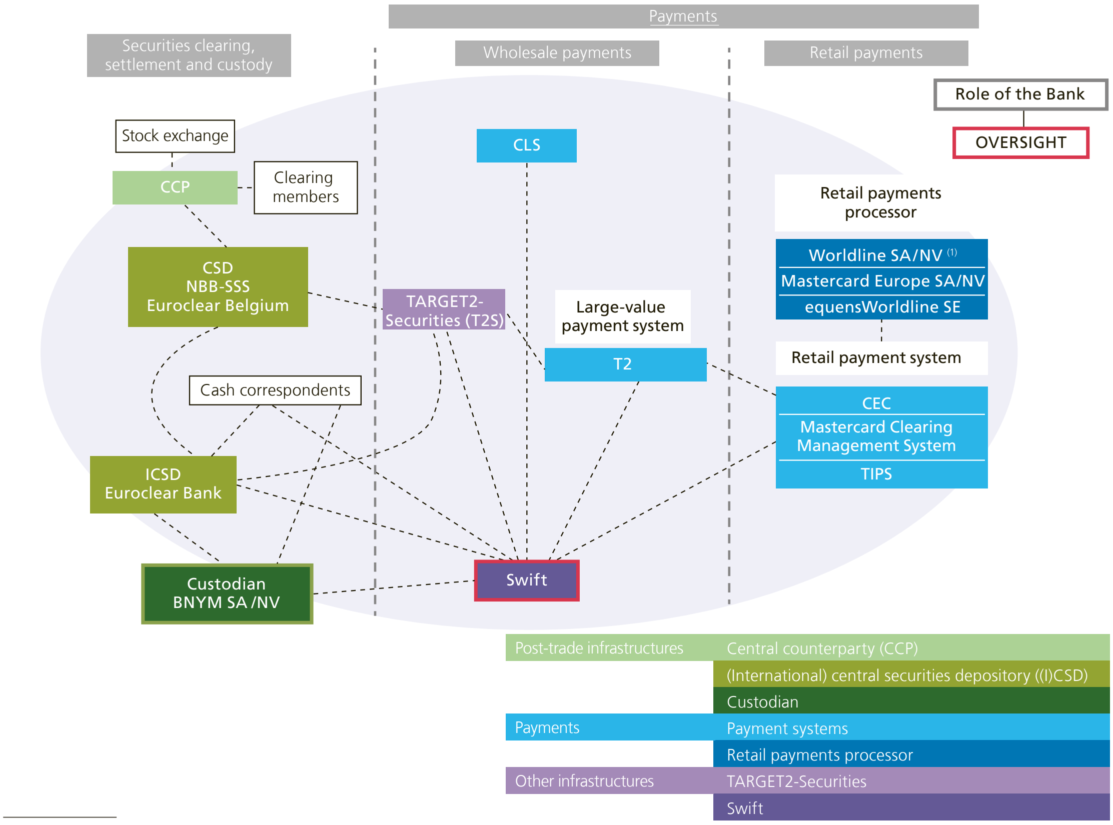
4. Swift

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 types of customers, which vary in terms of their size and activity, including banks, brokers, investment managers, fund administrators, custodians, corporates and Treasury counterparties. Swift is registered in Belgium, with its headquarters in La Hulpe.

Through its financial messaging services, Swift plays a crucial role in facilitating correspondent banking and financial market infrastructure operations. This fundamental role in the global financial sector creates significant systemic dependency on Swift. Hence, the G10 established a cooperative oversight framework to monitor Swift's activities with the aim of safeguarding financial stability.

Figure 4

Swift as a critical service provider to the financial industry



[1] Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland Ltd is also designated as a systemic processor for its switching activities for Bancontact according to the Act of 24 March 2017 on the oversight of payment processors but is not overseen by the NBB.

4.1 Swift oversight framework

4.1.1 Swift and its users

As a member-owned cooperative, Swift is owned and controlled by its users. To facilitate engagement and involvement, Swift's users are organised into National Member Groups. National Member Groups comprise all Swift shareholders in a country and propose candidates for election to Swift's board of directors. They act in an advisory capacity to the board of directors and Swift's management. The composition of Swift's board is designed to reflect the use of Swift messaging services, ensure its global relevance, support its international reach, and uphold its strict neutrality. A nation's use of Swift's messaging services determines both its Swift shareholding allocations and the number of board members to which it is entitled. Shares are reallocated based on the financial contribution of shareholders for network-based services. Since this factor varies over time, the shares are reallocated every three years to mirror actual usage of Swift messaging services. The next reallocation is scheduled to take place in 2024.

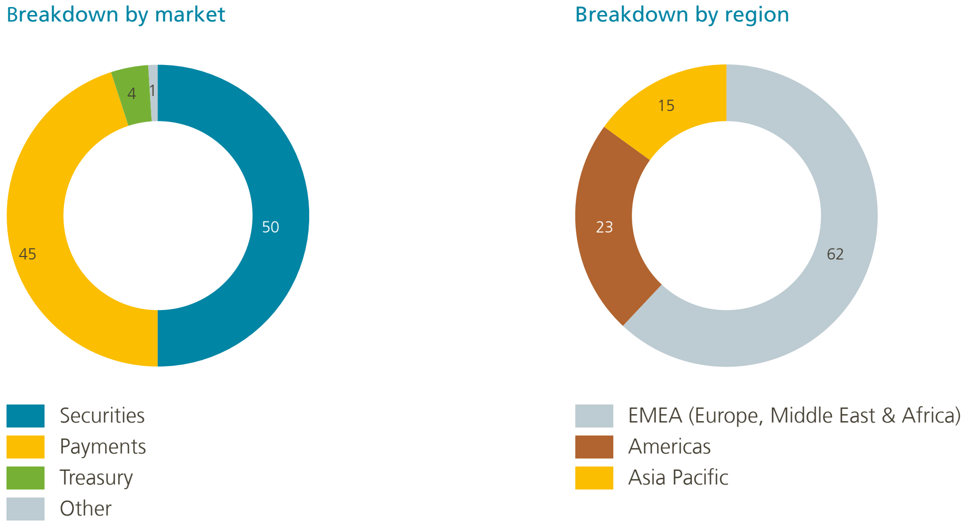
The following numbers reflect Swift's global reach and its important role in the global financial infrastructure. Swift provides messaging services to customers located in more than 200 countries, amounting to approximately 11 800 registered live users, of which 2 335 are Swift shareholders. In 2023, 11.9 billion messages were sent with a daily average of 47.6 million.

The core service for the exchange of financial messages is Swift's FIN application. The following figure shows FIN traffic for 2023 distributed by region and market, respectively. In line with figures for previous years, the payments (45 %) and securities (50 %) markets represented the lion's share of Swift's messaging traffic volumes in 2023. The Europe, Middle East and Africa (EMEA) region accounted for the largest share of total 2023 FIN traffic volume, followed by the Americas and the Asia Pacific region. It should be noted that the migration to ISO 20022 led to a revision of the calculation method for these results, resulting in FIN InterAct Payment flows being included in the payment metrics as from March 2023. Please see section 2.3 below for more information on the migration to ISO 20022.

Figure 5

Swift FIN traffic distribution by region and market

(2023)



Breakdown by market

Breakdown by region

Source : Swift.

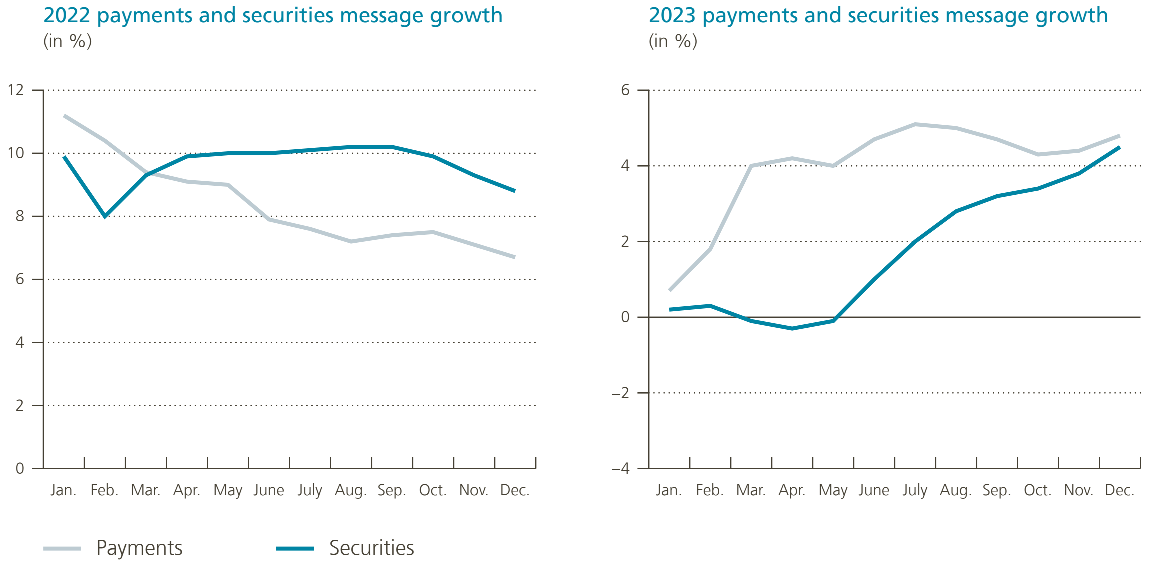
In 2023, despite numerous continuous challenges, such as a global economic slowdown, persistent inflation, turmoil on the financial markets and geopolitical instability, Swift reported positive growth in messaging traffic related to both payments (4.8 %) and securities (4.5 %) at year's end. These figures contributed to overall FIN traffic growth of 4.5 % for 2023.

The mild growth in securities traffic in 2023 (+4.5 %) was due to a slowdown in the first half of the year, attributed to reduced volatility and investment activity. On the other hand, the growth in payments in 2023 (+4.8 %) was on par with 2022, owing to sustained instruction volumes growth alongside test volumes for ISO 20022 migration. This was partly offset by a slowdown in reporting flows compared with historical averages.

The following two graphs show the percentage change in FIN payments and securities traffic for 2022 and 2023, respectively.

Figure 6

Growth in payments and securities messaging traffic in 2022 and 2023



Source: Swift.

4.1.2 International cooperative arrangement

In 1997, the G10 central banks[1] formalised the Swift oversight arrangement for the purpose of monitoring the adequate and safe functioning of this critical service provider. In addition to the participating G10 countries, the Bank for International Settlements and the European Central Bank are represented in the international working groups. As Swift is headquartered in Belgium, the Bank acts as lead overseer and chairs the international oversight meetings.

The G10 central banks are represented in four working groups: the Technical Group (TG), which conducts technical fieldwork; the Cooperative Oversight Group (OG), the decision-making body which sets oversight strategy; the Executive Group (EG), which serves as the interface for overseers to communicate conclusions and

[1] The G10 central banks involved in Swift oversight are the Bank of Canada, the Deutsche Bundesbank, the European Central Bank, the Banque de France, the Banca d'Italia, the Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, the Swiss National Bank, the 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.

recommendations to Swift's board and executive management; and the Oversight Forum (SOF), which brings together a wider group of central banks to discuss oversight activities and relevant changes at Swift.

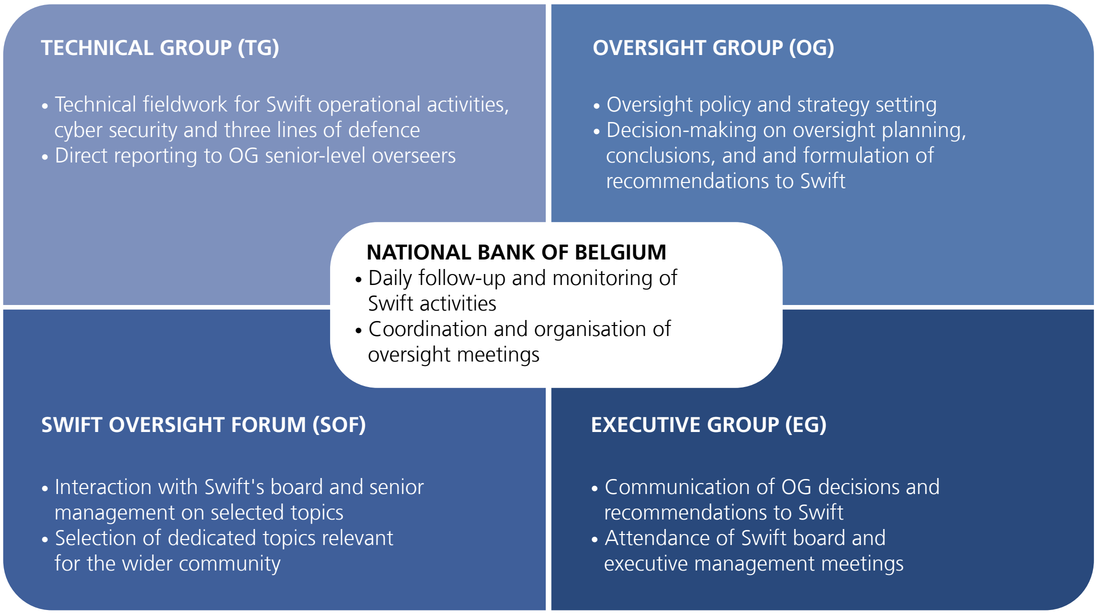
Given the systemic nature of Swift, a larger group of G20 countries are directly involved in oversight. These G20 central banks are represented in the SOF. Membership corresponds to their share of total Swift traffic volume and the CPMI membership composition. The SOF deals with Swift oversight conclusions, planning and priorities, the Customer Security Programme, and other specific topics. In-person meetings of the SOF will resume in 2024, following a temporary switch to virtual meetings to comply with statutory and regulatory public health requirements during the Covid-19 pandemic.

In its capacity as Swift's lead overseer, the Bank 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 Bank serves as the entry point for channelling information to the other overseers and, as chair, coordinates the various working groups in terms of reporting to the other overseers and preparing discussion items.

More information on the composition and activities of each working group, as defined in the current oversight framework, can be found in previous editions of this report (2017–2023). The figure below provides an overview of the working groups involved in the oversight of Swift.

Figure 7

Swift oversight working groups involving G10 and G20 central banks



TECHNICAL GROUP (TG)

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

OVERSIGHT GROUP (OG)

- Oversight policy and strategy setting
- Decision-making on oversight planning, conclusions, and and formulation of recommendations to Swift

NATIONAL BANK OF BELGIUM

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

SWIFT OVERSIGHT FORUM (SOF)

- Interaction with Swift's board and senior management on selected topics
- Selection of dedicated topics relevant for the wider community

EXECUTIVE GROUP (EG)

- Communication of OG decisions and recommendations to Swift
- Attendance of Swift board and executive management meetings

Source: Swift.

Oversight of Swift is based on five High-Level Expectations (HLEs), i.e. (1) Risk Identification and Management, (2) Information Security, (3) Reliability and Resilience, (4) Technology Planning, and (5) Communication with Users. These five HLEs are set out in Annex F to the CPMI-IOSCO's Principles for FMIs and form the oversight expectations applicable to all FMI critical service providers.

The activities of overseers are anchored in the five HLEs which drive their planning and priorities. Overseers assess the adequacy of Swift's management of operational and security risks across the three lines of defence, comparing it with these expectations. Swift is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. the provision of required documentation, interaction with Swift's three lines of defence, and discussions with executive management and the board).

More information on how the oversight activities for 2023 can be linked to each of the five HLEs can be found at the end of this section.

4.1.3 Changes to the Swift oversight arrangement

The Oversight Group (OG) is currently revising the oversight framework set out above. The current framework is based on a memorandum of understanding (MoU) concluded between Swift and the Bank, as well as additional MoUs concluded by the Bank with each G10 central bank directly involved in the oversight of Swift, including the European Central Bank. As mentioned above, the Bank has been designated the lead overseer of Swift.

The current oversight framework focuses primarily on various operational risks. As stated above, overseers have translated these operational risks into five High-Level Expectations (HLEs). Two HLEs focus on risk management (HLE 1, Risk Identification and Management, and HLE 5, Communication with Users) while three HLEs deal with the specific types of risks to be managed (HLE 2, Information Security; HLE 3, Reliability and Resilience; HLE 4, Technology Planning).

The use of HLEs provides Swift and its overseers with a common language and a framework within which discussions can be held and overseers can organise their activities. However, oversight discussions are not necessarily limited to topics included in the HLEs, as the oversight framework is broader and can encompass other specific topics for review and discussion with Swift's management and internal audit service.

The last major review of the oversight arrangement dates from 2005. Since then, the regulatory expectations of banking and financial market infrastructure overseers have evolved. For example, Basel III introduced new capital requirements for the banking sector, while the CPMI-IOSCO Guidance on cyber resilience, the Eurosystem's Cyber resilience oversight expectations for financial market participants and Regulation (EU) 2022/2554 on digital operational resilience (DORA) have resulted in changes to expectations with regard to operational risks.

Although these regulations and guidance are not directly applicable to Swift as it is neither a bank nor a financial market infrastructure, Swift's top-tier overseers are of the view that several of these expectations should be codified so as to function as a legal backstop and ensure a level playing field for oversight and supervision of the financial sector. The proposed review of the oversight framework focuses on the importance of Swift as a critical provider of messaging services to the financial sector and recommends aligning the expectations of overseers with customary expectations in the broader financial sector, such as the CPMI-IOSCO Principles for financial market infrastructures (PFMI), whilst taking into account the specific nature of Swift.

The intention of overseers is not to change the content or objectives of the current oversight framework fundamentally, but rather to codify particular aspects of this framework so that it can serve as a legal backstop.

The current organisation of and approach to Swift oversight will be maintained, including the two-tier structure with a technical (TG) and senior-level (OG) oversight body. The revised approach will also seek to maintain collaborative, consensus-building interaction amongst overseers at both the technical and senior levels.

As Swift is a cooperative company under Belgian law, a legislative proposal to be brought before the federal Parliament will be developed, after a consensus is reached on its content within the Oversight Group.

4.2 Selection of major topics analysed by overseers in 2023

A non-exhaustive selection of major topics which overseers analysed in 2023 is presented below. The highlighted topics are not a full representation of the review work conducted in 2023 (e.g. standing topics such as business continuity exercises, effectiveness of the three lines of defence, enterprise risk management and internal audit activities).

4.2.1 Cyber- and physical security

In 2023, oversight work continued to be carried out against the backdrop of the high geopolitical uncertainty that first arose in 2022. As Swift is essentially an ICT company, cyber and physical security is a major focus area for overseers.

Cybersecurity is a broad term that encompasses various fields, each of which focuses on specific aspects of digital security. Managing these fields is crucial to ensuring both security and operational resilience, as they collectively contribute to protecting Swift's information, systems and networks against cyber threats. The areas covered include governance and risk management, identity and access management, application security, data security, incident and response management, and cloud security. Due to their importance and contribution to Swift's overall security posture, these are standing items on the oversight agenda.

One emerging issue in the area of cybersecurity is quantum cryptography, or the leveraging of principles of quantum mechanics to perform cryptographic tasks, such as data encryption, and ensure the security of communication channels.

From an oversight perspective, monitoring the development of Swift's quantum cryptography capabilities is aligned with the objectives of long-term security planning and maintaining data confidentiality, so as to future-proof the environment in which Swift operates and ultimately ensure trust in the global financial sector.

Another topic that attracted the attention of overseers was third-party risk management (TPRM), sometimes referred to as "supply chain risk management" or "vendor risk management". This was covered in depth by way of an on-site review (OSR) in 2023. For more information on the context and outcome of the OSR, please see Box 8.

Physical security is a critical part of an organisation's overall security posture and, in conjunction with cybersecurity measures, helps provide a comprehensive defence against various threats. While cybersecurity focuses on protecting digital assets and information, physical security addresses the safeguarding of tangible assets, facilities and personnel. Accordingly, topics such as asset protection and the physical security of Swift's data centres and operating locations, the prevention of unauthorised access, business continuity, and resilience and disaster recovery are recurring items on the oversight agenda.

Overseers can organise on-site visits to Swift's offices and locations to further assess its compliance with their expectations in terms of cyber and physical security. Such visits allow overseers to gain insight into the company's operations, including its organisational culture, compliance with technical and security controls, and overall security posture.

BOX 8

On-site review of third-party risk management

The Oversight Group (OG) decided to conduct an on-site review (OSR) in 2023 on the topic of third-party risk management (TPRM) to examine Swift's TPRM practices, policies and procedures and assess whether they adequately meet oversight expectations. Third-party risks refer to those that arise from the use of third-party vendors, suppliers or service providers. These risks can be grouped into several categories, including financial risks, operational risks, cybersecurity risks, business continuity risks and reputational risks.

An example of cyber risk is a supply chain attack. This is an attack on an organisation's suppliers in order to gain unauthorised access to its systems or data. The damage from such an attack can be substantial. Supply chain attacks can be carried out through, among other means, compromising software patches or updates, undermining code signing or manipulated open-source code. A disproportionate reliance on start-up suppliers can also pose a risk as the business model and security practices of newly established companies have yet to prove their effectiveness over time.

The Covid-19 pandemic exacerbated the operational risks faced by financial institutions in relation to the rapid adoption of, and increased dependency on, ICT infrastructure and the sector's growing reliance on technology-based services provided by third parties, of which cloud service providers are a prime example.

The Bank for International Settlements therefore noted that attention should be paid to the appropriate management of third- and fourth-party relationships and concentration risk exposures so as to enhance the ability of financial institutions to withstand, adapt to and recover from potential hazards and mitigate potentially severe disruptive events.[1]

In addition, in this context, the EU took steps to codify certain expectations with regard to third- party risk management in regulations such as the Digital Operational Resilience Act (DORA).

Swift is in the process of updating its vendor risk management processes and practices to keep pace with these developments. Overseers wish to learn more about the actions proposed by Swift to improve its processes and practices. More specifically, they are interested in how Swift currently approaches issues such as the management of third parties, vendor lifecycle management, vendor categorisation, the mitigation of third-party risks, and business continuity as well as changes planned for the future. Against this backdrop, third-party risk management was selected as the focus area for the 2023 on-site review.

In preparation for the on-site review, overseers examined numerous practices and guidelines relating to third-party risk management. Documents provided by Swift were also reviewed to gain insight into existing policies and practices.

The on-site review was carried out over the course of one week, with support from a number of representatives of other central banks. As third-party risk management is a very broad topic, it was

[1] See https://www.bis.org/publ/bcbs_nl28.htm.

necessary to interview various people at Swift from different departments, either in-person at Swift's headquarters or virtually, for functions based abroad.

Following the on-site review and taking into account the documents provided and information gleaned from the interviews, the OSR team formulated a number of observations on areas in which improvements could be made. These observations were compiled in a report which was approved by the OG and provided to Swift. Follow-up of the actions undertaken to address these observations will form part of the oversight work carried out in 2024.

4.2.2 Customer Security Programme

Swift's Customer Security Programme (CSP) has been a recurring topic on the agenda of overseers since its introduction following the 2016 Bangladesh bank heist. Swift has created an extensive programme to enhance the cybersecurity of users, their counterparts and the community as a whole. Through the CSP, users are required to adhere to certain controls and good practices to secure appropriately their on-site ICT environments connected to the Swift network. With cyber-attacks on the rise in the financial sector, overseers seek reasonable assurance as to 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 its CSP, such as an annual review of its Customer Security Control Framework (CSCF), improvements to the know-your-customer (KYC) tool, the launch of an Independent Assessment Framework (IAF), the introduction of compulsory assessments, more effective involvement of supervisors, actionable updates to the Information Sharing and Analysis Centre (ISAC), and the organisation of recurring awareness campaigns. Thanks to these actions, Swift informed overseers that there has been a downward trend in customer incidents. In fact, since the beginning of 2021, not a single customer incident involving the transmission of a fraudulent message over the Swift network has been reported. Due to the programme's successful track record and promising results, Swift is expected to continue enhancing it.

One expectation concerns the involvement of supervisory authorities in the use of CSCF self-attestation data from financial institutions. From the outset, overseers have encouraged Swift's move to engage supervisors more directly in making effective use of its users' rich self-attestation data, which could provide crucial input for supervisors' risk-based planning and scoping. However, the identification and onboarding of the relevant supervisory authorities in the know-your-supervisor (KYS) tool have proven challenging as, in some cases, multiple supervisory authorities are responsible for a single country. According to Swift's initial reporting to overseers, the use of self-attestation data by onboarded supervisory authorities for financial institutions within their relevant jurisdictions has fallen short of expectations. Overseers have stressed the importance of this initiative and will continue to monitor the actions taken to improve supervisory onboarding and safeguard the effectiveness of the KYS application.

As per standard procedure, overseers contributed, together with the National Member Groups, to the annual review of the Swift Customer Security Control Framework (CSCFv2024), which resulted in one advisory control being made mandatory as well as a number of other changes to the framework :

i. Raising of control 2.8 (Outsourced Critical Activity Protection) from advisory to mandatory to support the ramp-up of outsourcing and use of cloud computing in the community.

ii. Changes to control 2.4A (Back Office Data Flow Security) as well as clarifications and cosmetic changes to improve usability and the implementation of controls.

Swift users are expected to comply with the mandatory controls (i.e. the security baseline) and can certify their compliance with the advisory controls (i.e. good practices for securing local ICT infrastructure) by uploading an attestation (i.e. regarding compliance with the CSCF security controls) using the Know-Your-Customer Self-Attestation (KYC-SA) tool. A new version of the CSCF (v2024) was introduced in mid-2023. Users have until the end of 2024 to submit their attestations.

As of 31 December 2023, 86 % of Swift customers had provided a valid CSP attestation, with 84 % indicating compliance with all mandatory controls. The compliance levels and the number of self-attestations are in line with the uptake in 2021 and 2022. Through Swift's quality assurance and monthly metrics reports, overseers closely monitor various CSP-related variables, such as user attestation and consultation levels. 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 CSP reporting metrics as appropriate.

The Independent Assessment Framework (IAF), which was launched in mid-2021, requires all Swift users to perform a Community Standard Assessment to further enhance the accuracy of their attestations. Every Swift user must have their attestations independently assessed by either an internal independent assessor (e.g. the second or third line of defence) or an external independent assessor (such as a consultancy firm). Users are free to select the internal and/or external resources to be used to conduct this assessment. If a user opts for self-attestation without an independent internal or external assessment, they will be considered non-compliant with the CSP.

Initial reporting on the IAF is in line with that of previous years, with 93 % of users opting for an independent assessor and thus compliant with CSP requirements. Of these users, about half opted for independent internal assessment and half for independent external assessment. The percentage of Swift traffic sent by BICs that provide attestations supported by an independent internal or external assessment is fairly stable at 99 %.

A new addition to the CSP framework was Customer Security Programme Assessor Certification (CSPAC). Swift launched this programme in mid-2023 to address a number of challenges faced by the community in adhering to the IAF, such as scope creep and cost overrun, and in response to requests by customers for a trusted list of certified assessors. These issues were primarily due to gaps in the standardisation of deliverables and inconsistent quality in terms of assessor activity. By means of the CSPAC, Swift aims to raise the expertise of independent assessors, standardise the CSP assessment methodology, and formalise the key outcomes of an independent CSP assessment.

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

4.2.3 ISO 20022 migration and transaction manager

In 2023, the financial sector started migrating to ISO 20022, an open global standard for transferring financial messages and information. The new standard provides consistent, rich and structured data that can be used for all kinds of financial transactions. The migration of Swift's user community to this new standard began over the weekend of 18-19 March 2023, when cross-border payments and reporting (CBPR+) traffic and a number of market infrastructures, including the Eurosystem's T2 Real-Time Gross Settlement (RTGS) system, EBA Clearing's EURO1 high-value payment system, Australia's Reserve Bank Information and Transfer System (RITS), New Zealand's Exchange Settlement Account System (ESAS), and Canada's Lynx high-value payment system were successfully migrated. In June 2023, the UK's CHAPS and the Bank of England's RTGS system followed suit.

Other market infrastructures, such as the Clearing House Interbank Payments System (CHIPS) and Fedwire, the funds transfer system operated by the US Federal Reserve Banks, will migrate at a later date.

To facilitate the further rollout of ISO 20022 across institutions and jurisdictions worldwide, Swift allows for a co-existence period. This period, during which users are expected to switch from the legacy FIN MT format to the new ISO 20022 MX format, started in March 2023 and is scheduled to end in November 2025. At the end of the third quarter of 2023, ISO 20022 migration for CBPR+ represented around 16 % of total traffic volumes since the start of the coexistence period. Combined with Swift Payments Market Infrastructure (PMI) traffic, the total percentage of payments traffic in ISO 20022 represents 35 %.

As a global standard setter, Swift takes the lead in coordinating ISO 20022 migration for its community. Since the start of this project, overseers have closely monitored Swift's approach, project management and planning, risk assessment and communication with users. They will continue to follow up on Swift's initiatives to facilitate timely migration to the new standard within the coexistence window.

Swift's Transaction Manager (TM) platform is closely related to ISO 20022. In 2019, Swift revealed plans to develop this platform in a push to move away from traditional sequential messaging to a system that allows every participant in a transaction to have an end-to-end and up-to-date view on the status of the transaction. In addition to operational advantages, the TM platform will play an important role in supporting financial entities that have not completed migration to ISO 20022 by the end of the coexistence period.

By moving from secure message forwarding to end-to-end transaction management, Swift wishes to use richer data and reduce friction (i.e. provide a better customer experience, enhance efficiency and include value-added services such as transaction validation). The underlying communication channel for a transaction is format agnostic and can be FIN MT, ISO 20022 MX, or a combination of channels based on the capabilities of the transaction parties involved (i.e. backward compatibility). The platform ensures full transaction data accessibility to any authorised party in the transaction chain, thereby helping to ensure end-to-end transparency. In the future, Transaction Manager may also help facilitate the use of application programming interfaces (APIs) so that authorised users can retrieve the status of their transaction via an API call over the Swift network.

Swift's Transaction Manager went live in November 2022 and started processing live customer traffic in May 2023. By the end of September 2023, full-service availability had been achieved, with 100 % of ISO 20022-originated payments being processed by Transaction Manager.

4.2.4 Swift's contribution to the G20 roadmap for enhancing cross-border payments

In 2020, the G20 announced the Roadmap for Enhancing Cross-border Payments, which includes several actions to improve the speed, cost, transparency, choice of and access to cross-border payments. From the outset, Swift supported the objectives set out in the roadmap in several ways.

One example is the aforementioned industry-wide migration to ISO 20022, launched in March 2023, which is setting the stage for new levels of operational efficiency and innovation. In fact, Swift's Payments Market Practice Group (PMPG) was directly involved in a workstream focused on improving data quality and straight-through processing by enhancing data and market practices. The adoption of a common message format, such as ISO 20022, should play an important role in ensuring payment system interoperability and, more generally, in addressing data standards and quality and quantity restrictions in cross-border payments.

A joint task force consisting of banks and financial market infrastructures, sponsored by the PMPG, has developed preliminary harmonisation guidelines with the aim of setting minimum requirements for core data components across the cross-border payments chain. These guidelines could serve as best practice requirements for ISO 20022 messaging in cross-border payments after the co-existence phase ends in 2025.

According to analysis of payment exceptions by Swift, formatting issues, account issues and invalid data are major sources of friction in the area of cross-border transactions. Much of this friction could be avoided by checking payments for errors before they are sent. To that end, Swift offers Payment Pre-validation, a service that allows users to check for typos and formatting errors upfront to ensure payments go through the first time. This service continued to gain momentum in 2023, with around 300 financial institutions having signed up.

Launched in 2017, the Swift Global Payments Initiative (GPI) gained traction as the new standard for cross-border large value payments. Swift GPI combines traditional Swift messaging with a new set of rules. Any financial institution adhering to the GPI has to follow these rules, which provide for transparency of fees, end-to-end payment tracking, and confirmation of credit to the recipient's account. Each transaction is assigned a unique end-to-end transaction reference (UETR) which payment providers can use to trace the transfer from start to finish.

The benefits for GPI customers are numerous. Firstly, GPI substantially increases payment speed by eliminating payment friction and reducing the risk of delays through upfront account verification. Another way GPI reduces friction is through automated exception management processes, allowing users to handle queries between banks on the Swift network and resolve instances of incorrect or missing payment information.

Financial crime compliance (FCC) is another important aspect for participants in cross-border transactions. FCC offers a portfolio of financial crime compliance solutions that help member institutions navigate more complex compliance requirements.

As such, GPI fits into Swift's strategy of ensuring fast and frictionless messaging services. As the benefits of GPI are realised leveraging Swift's existing messaging infrastructure, users can expect the same level of security and resilience as when using traditional Swift messaging services.

Whereas Swift GPI facilitates high-value or wholesale cross-border payments, Swift Go aims to ensure fast and frictionless low-value international payments, another key objective of the G20 roadmap. Introduced in July 2021, Swift Go 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. It allows sending banks to fully customise their front end to offer customers an easy and intuitive payment experience. As such, Swift wishes to ensure that the traditional banking sector remains competitive in the high-growth market for low-value cross-border payments.

Swift Go builds on the rails of Swift GPI to facilitate speedy cross-border payments. It leverages enhanced service levels between banks, a single payment format and pre-validation services, ultimately removing delays caused by friction in the transaction chain. In addition to faster payments, Swift Go offers more competitive processing fees, enhanced transparency, greater predictability, and payment tracking, combined with the security that users have come to expect from Swift. More than 600 customers had already signed up for Swift Go, with more than 450 banks testing the service or technically live, at the end of 2023.

The services and products outlined above illustrate Swift's eagerness to support the industry's push towards enabling faster, cheaper, more accessible and transparent payments. Swift is continuously examining and developing advanced capabilities for its service offering for both payments and securities, improving end-to-end transaction processing and helping banks and financial institutions deliver the high-quality services their customers expect.

In September 2023, Swift announced that it would introduce Swift Essentials, a portfolio of value-added services, including GPI, Swift Go, Pre-validation, Swift Transaction Screening and Swift Payment Controls. Since 1 January 2024, Swift Essentials has been universally applied to all Swift users in scope, entitling them to take up any components or value-added services in the portfolio, with a single annual invoice issued for all services included in Swift Essentials.

To properly inform its user community, Swift conducted a Swift Essentials awareness campaign throughout 2023, reaching out to the community and specific clients.

4.3 Focal points for Swift oversight in 2024

The annual planning of Swift oversight is guided by a risk-based approach. The oversight risk assessment is intended to help maximise the effectiveness and efficiency of the review. The 2023 assessment was used as a basis for 2024 planning. After each quarter, overseers evaluate the topics analysed and decide which require deeper review or possibly additional information from Swift. This approach gives overseers the flexibility to dedicate more time to particular topics, where appropriate, or to coordinate follow-up discussions at a later stage.

Swift operates in a changing environment characterised by increasing competition and rapidly evolving technologies. This context affects its go-to-market strategy (e.g. new product offerings and a shift towards agile software development) and operations (e.g. the software development lifecycle, incident management and business continuity). Furthermore, an appropriate strategy should be set to tackle a range of emerging challenges, such as geopolitical issues, 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 assessment, security decisions and design choices, while keeping the global user base properly informed. Overseers seek assurance at all times that the risks identified as arising from new technology choices and major projects are adequately managed and mitigated, to ensure business continuity with comparable or better resilience.

Cybersecurity strategy and risk management remain major topics on the agenda of overseers for 2024. Overseers are analysing which security investments and enhanced capabilities will contribute to protecting Swift against increasingly sophisticated cyberattacks. The cybersecurity review also entails challenging the ISAE 3000 reports by Swift's external security auditor. These reports provide independent assurance on Swift's internal policies, procedures and controls structured around the five sets of HLEs. The ISAE 3000 reports include rich information important to the oversight of Swift and are thoroughly reviewed each year.

The software development lifecycle (SDLC) is intricately connected to both security and operational resilience within an organisation. Throughout the various phases of the SDLC, security measures can be integrated to identify and address vulnerabilities, ensuring that customer-facing product offerings developed by Swift are resilient to potential threats. By incorporating security considerations such as requirements and design as early as possible, organisations can proactively mitigate risks and enhance the overall security posture of their systems.

Change management is another closely related topic. Change management processes are designed to control and manage modifications to the ICT environment, which is essential to maintaining secure and stable infrastructure. Change management relates to the focus on implementing alterations to software after its initial release as changes introduced during the software development process require careful consideration to avoid disruptions, maintain system integrity, and ensure alignment with organisational goals. Proper oversight is crucial to the collective monitoring of these processes as it ensures that changes are systematically evaluated, approved and integrated into the software, thereby preventing potential issues and guaranteeing stability, security and functionality.

Due to a slight uptick in service availability-related issues in the recent past, overseers will continue to monitor and refine policies and processes related to problem and incident reporting by Swift.

Follow-up of the CSP is also on the oversight agenda for 2024. The Swift user community's level of compliance with CSCF controls, developments concerning customer cases, the results of the new cycle of mandatory independent assessments, and the CSPAC initiative are of particular interest from an oversight perspective. The Bank, in its capacity as lead overseer, will use the in-person Swift Oversight Forum meeting to provide an update on the proposed changes to the CSCF. In doing so, the overseers seek to encourage other national authorities and supervisors to continue to push supervised institutions to improve their endpoint security and to leverage the capabilities of KYS self-assessment data in their oversight toolbox.

Finally, the outcome of the OSR of third-party risk management resulted in a few observations which will require Swift to take appropriate follow-up actions. The TG will monitor the implementation of these actions and mitigating measures in the coming year. Swift has defined new processes to monitor third-party risks based on recently published best practices. The gradual migration of its existing (critical) vendor base to the new approach will be a focus area for TG activities in 2024.

Oversight planning for 2024 is structured around the five HLEs, which serve as the starting point when selecting topics for review. In accordance with the risk-based approach, the previous year's assessment forms the basis for the coming year's review activities. For 2023, this resulted in an extensive list of topics to be analysed by overseers, of which the major ones were:

- HLE 1: Risk Identification and Management
    - Swift's overall risk profile and topic-specific risk assessments
    - Development of an enterprise-wide governance risk & compliance tool
    - Internal and external audit findings and identified mitigating actions

- HLE 2: Information Security
    - Data confidentiality, integrity and availability, including the quantum cryptography roadmap
    - Threat-led penetration test (red-team) outcomes

- HLE 3: Reliability and Resilience
    - Incident management and business continuity
    - Implementation of change management practices

- HLE 4: Technology Planning
    - ICT technology roadmap and investment drivers
    - New product and service offerings and collaboration between Swift and the industry

- HLE 5: Communication with Users
    - Outreach to the global user community
    - Appropriate collaboration with the global user base to increase the resilience of end-users