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 and headquartered in La Hulpe.

Through the provision of 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 for the purpose of safeguarding financial stability.

4.1 Swift oversight framework

4.1.1 Swift and its users

Swift is a member-owned cooperative, meaning it is owned and controlled by its users. In order to use Swift's messaging services, an entity must be registered as an authorised Swift user in one of the following categories: supervised financial institutions, non-supervised financial entities active in the financial industry, and closed user groups and corporate entities. Institutions that use Swift's services may be considered for admission as Swift shareholders, with the number of shares to be allocated determined based on their usage of these services. This shareholder structure ensures that Swift's governance reflects the collective interests of its users and fosters transparency, inclusivity and a shared commitment to the platform's development and global financial stability.

Swift's National Member Groups and National User Groups help provide a coherent global focus by ensuring a timely and accurate two-way flow of information between Swift and its users. National Member Groups consist of all Swift shareholders in the same country and represent the local shareholder community to Swift. National User Groups comprise all Swift users in the same country and act as a forum for the discussion of operational matters.

Swift provides messaging services to customers located in more than 200 countries and territories, amounting to approximately 11 800 registered live users, of whom approximately 2 400 are Swift shareholders. In 2024, 13.4 billion messages were sent, with a daily average of 53.3 million. These figures reflect Swift's global reach and its important role in the global financial system.

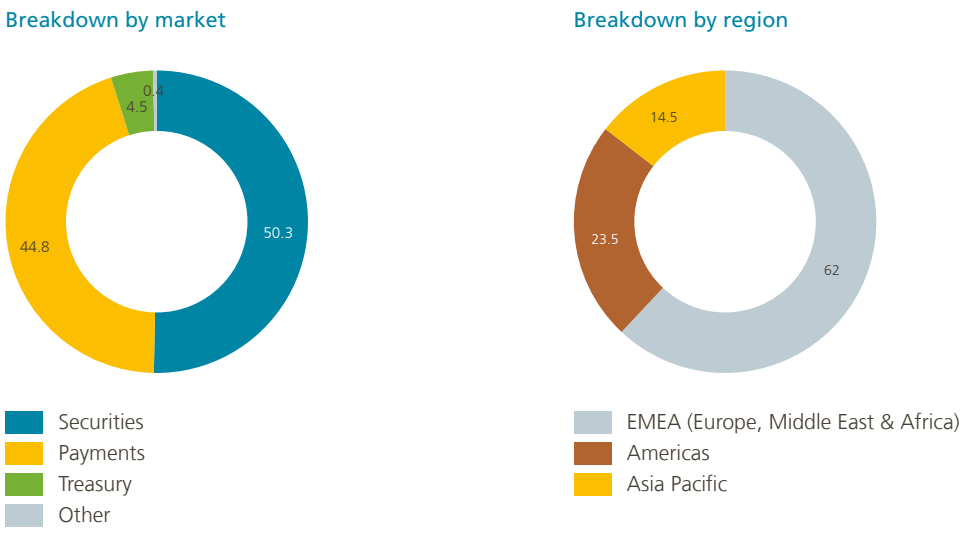
Swift's core service for the exchange of financial messages is FIN. The following charts show Swift's FIN traffic for 2024 distributed by market and region. In line with figures for previous years, the payments (44.8%) and securities (50.3%) markets represented the lion's share of Swift's messaging traffic volume for 2024. Europe,

the Middle East and Africa (EMEA) accounted for the largest share of 2024 FIN traffic volume by region, followed by the Americas and the Asia Pacific region. It is important to note that migration to ISO 20022 led to revision of the method used to calculate these results, resulting in FIN InterAct flows being included in the payments figures as from March 2023. Please see section 2.3 below for more information on the migration to ISO 20022.

Figure 10

Swift FIN traffic distribution by market and region

(2024)



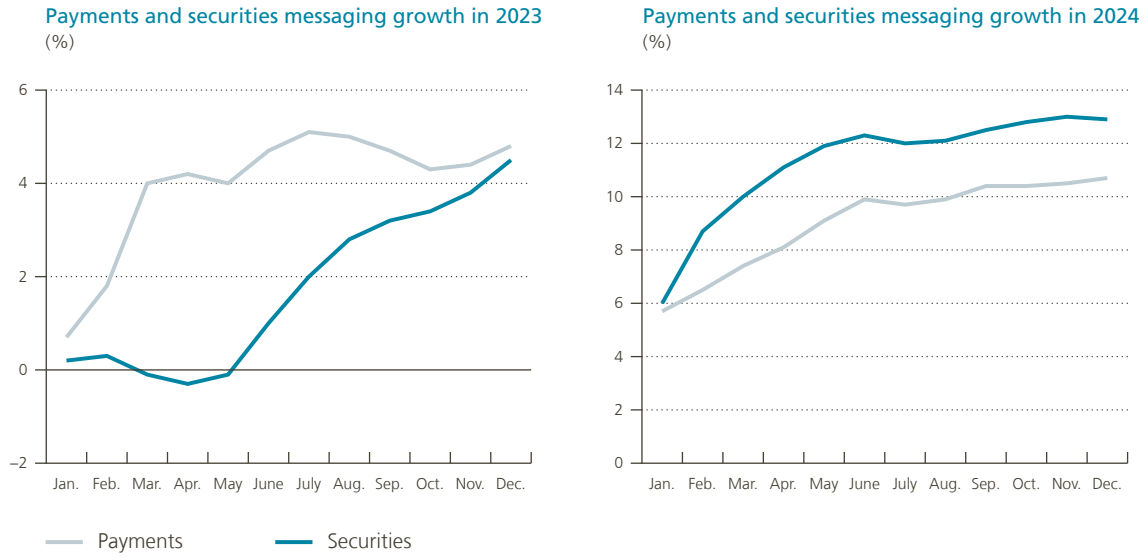
Source: Swift.

In 2024, Swift traffic grew at a higher rate than expected, with an average daily increase in FIN traffic of 12.1%, mainly driven by growth in securities (12.9%) and payment (10.7%) volumes. Swift attributes this growth to better than planned macro trends, as well as to business gains from a few top customers.

The following two graphs show the percentage change in FIN & InterAct payments and securities traffic growth in 2023 and 2024, respectively.

Figure 11

Growth in payments and securities messaging traffic in 2023 and 2024



Source: Swift.

4.1.2 International cooperative oversight arrangement

In 1997, the G10 central banks[1] formalised an oversight arrangement for Swift, to ensure the adequate and safe functioning of this critical service provider. The Bank for International Settlements and the European Central Bank are also represented in the Swift oversight 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 on all four Swift oversight working groups: the Technical Group (TG), which conducts fieldwork; the Cooperative Oversight Group (OG), the decision-making body responsible for determining oversight strategy; the Executive Group (EG), which communicates the overseers' conclusions and recommendations to Swift's board and executive management; and the Swift Oversight Forum (SOF), which interacts with Swift's management on selected topics.

Due to Swift's systemic importance, the Swift Oversight Forum (SOF) was established, involving a broader group of central banks. This body serves as a forum for the G10 central banks to share information on Swift oversight activities with a wider group of (G20) central banks. Membership corresponds to a country's share in total Swift traffic volume and to the CPMI membership composition. The SOF deals with Swift oversight conclusions, planning and priorities, the Customer Security Programme (CSP) and selected topics.

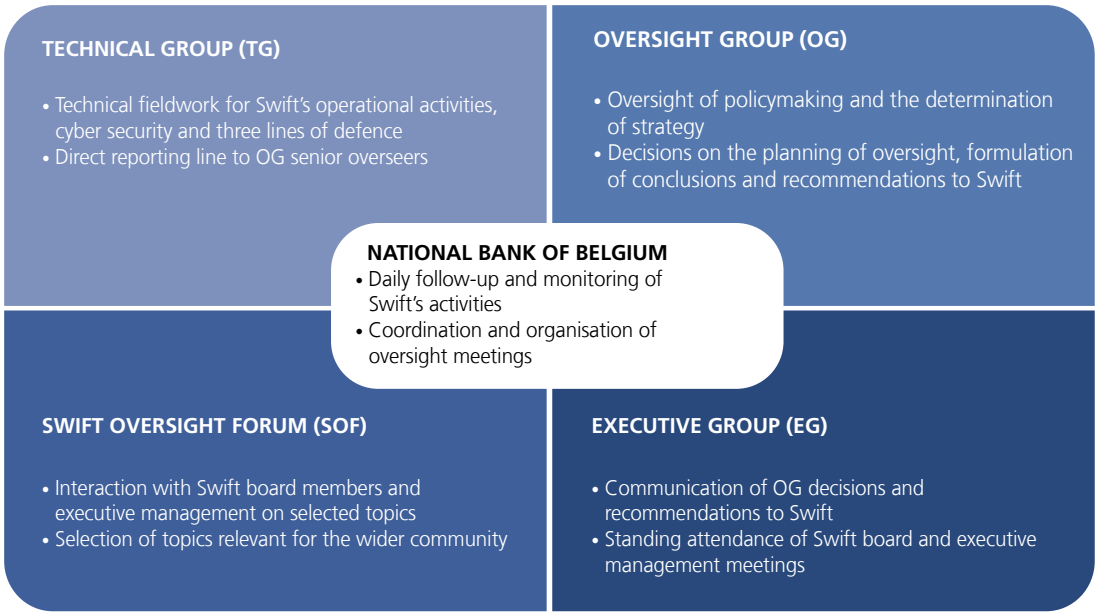
In its capacity as Swift's lead overseer, the Bank has a dedicated team which conducts daily monitoring and follow-up of Swift's activities and projects. As stated in the Swift oversight protocol, the Bank serves as the entry point for channelling information to the other overseers and, as chair, coordinates reporting by the different working groups to the other overseers and the preparation of items for discussion.

1 The G10 central banks involved in Swift oversight are the National Bank of Belgium (as lead overseer), 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, the 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.

The figure below provides an overview of the working groups involved in the oversight of Swift. Additional information on the composition and scope of activities of each working group, as defined in the current oversight framework, can be found in previous issues of the Financial Market Infrastructures and Payment Services Report (2017 – 2023).

Figure 12

Swift oversight working groups involving G10 and G20 central banks



Source: NBB.

Oversight of Swift is based on the High-Level Expectations for the Oversight of Swift (HLEs). The expectations relate to: (i) risk identification and management, (ii) information security, (iii) reliability and resilience, (iv) technology planning and (v) communication with users. The HLEs are set out in Annex F to the CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMIs) and form the oversight expectations applicable to all critical service providers.

The HLEs drive oversight planning and priorities. Overseers assess the adequacy of Swift's management of operational and security risks across its three lines of defence (LoD) with reference to these expectations. Swift is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. the provision of requested documentation, interaction with Swift's three lines of defence, and discussions with executive management and the board).

Additional information on 2024 oversight activities relating to the HLEs can be found at the end of this section.

4.1.3 Belgian law on the oversight of financial messaging service providers

Financial messaging service providers such as Swift play a crucial role in the functioning of financial systems, including clearing, settlement and payment systems.

As indicated above, the oversight activities carried out by the Bank as lead overseer, together with other central bank members of the Oversight Group (OG), are based on the non-binding High-Level Expectations for the Oversight of Swift, which rely on voluntary cooperation and adherence by the institution.

The last major review of the Swift oversight framework, which led to an update of the protocol between Swift and the Bank, dates back to 2004. Given the constantly changing environment in which Swift operates, the OG deemed it time to conduct an in-depth review. The overseers identified the following key changes to the operating environment:

Regulatory environment: There is a global trend towards codifying oversight arrangements to enhance their efficiency and effectiveness. Examples include the Eurosystem's Regulation on oversight requirements for systemically important payment systems (SIPS) of 3 July 2014, which translates the Principles for Financial Market Infrastructures (PFMIs) into hard law. Similarly, the European Market Infrastructure Regulation (EMIR) and the Central Securities Depositories Regulation (CSDR) transposed the PFMI-based oversight framework for CCPs and CSDs into EU law in 2012 and 2014, respectively. At the national level, the Belgian Act of 24 March 2017 formalised oversight expectations for payment processors.

The CPMI and IOSCO have issued guidance on the cyber resilience of financial market infrastructures while the European legislature has put in place a stronger statutory basis for the oversight of digital operational resilience (the Digital Operational Resilience Act or DORA).

Geopolitical environment: Swift operates in an increasingly multi-polar world characterised by de-globalisation. The current model of moral suasion will reach its limits should Swift no longer cooperate on a voluntary basis with requests by the Oversight Group.

Technological environment: While in 2005 Swift relied largely on proprietary software, there is a clear trend to integrate standardised technologies which could increase the organisation's attack surface.

Competitive environment: Swift has expanded its product offering beyond services related to secure messaging for correspondent banking or supporting payments and securities transactions for banks and FMIs, to include for example financial crime and compliance services, a retail payments space (Swift Go) and an instant payments platform. These products remain in line with Swift's objective of supporting its members, but face competition from other providers.

The overseers therefore decided to codify certain principles and standards to provide a statutory safety net and ensure a level playing field, in terms of oversight, with other major actors in the financial sector. The proposed revision of the oversight framework acknowledges the importance of financial messaging service providers to the financial ecosystem.

The OG used the CPMI-IOSCO's PFMIs as the basis for the codified oversight framework, in addition to Annex F to the PFMIs, which underpins current oversight. Even though Swift is not a financial market infrastructure, the OG determined that the oversight objectives set out in the PFMIs are relevant to the oversight of Swift.

The following PFMIs have been identified as relevant for systemically important financial messaging service providers: Principles 1 (legal basis), 2 (governance), 3 (framework for the comprehensive management of risks), 15 (general business risk), 16 (custody and investment risks), 17 (operational risk), 18 (access and participation requirements), 22 (communication procedures and standards), and 23 (disclosure of rules, key procedures, and market data).

For the interpretation of Principle 17 (operational risk) and the CPMI-IOSCO Guidelines on cyber resilience for financial market infrastructures, the overseers referred to the provisions of Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA) to ensure that these standards are met or exceeded.

Regarding the concrete translation of PFMI Principle 2 (governance), the prudential legislation applicable to institutions supervised by the Bank served as a model. The Act of 25 April 2014 on the legal status and

supervision of credit institutions (the Banking Act) was the main reference text, but other prudential laws were considered where they better aligned with the oversight objectives for systemically important financial messaging service providers, with adjustments made where necessary to reflect the specific legal status and activities of these entities.

The current organisation of Swift oversight will, however, remain unchanged, with the statutory framework primarily serving as a backstop. The collaborative, consensus-based interaction between overseers at both technical and senior levels will therefore not be affected.

The bill was discussed and approved at senior level within the Oversight Group and by the governors of the G10 central banks. It was voted into law in April 2025.

4.2 Key oversight issues in 2024

A non-exhaustive selection of key issues dealt with by overseers in 2024 is presented below. The highlighted issues do not represent the entirety of the review work conducted in 2024, as standing topics such as business continuity, the effectiveness of the three lines of defence, enterprise risk management and internal audit are excluded.

4.2.1 Cyber and physical resilience

Cybersecurity is a broad term that encompasses various fields, each of which focuses on specific aspects of digital security. Managing these domains is crucial to ensuring operational resilience, as they all contribute to safeguarding Swift's information, systems and networks from cyber threats. These domains 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 topics on the oversight agenda.

One emerging issue in the area of cybersecurity is post-quantum cryptography, which addresses the future threats posed by quantum computers to current encryption methods. Quantum computers, if sufficiently advanced, could break widely used public-key cryptographic systems, which are critical to secure digital communications and financial transactions. Post-quantum cryptography involves developing and implementing encryption algorithms resistant to quantum attacks, ensuring the long-term security of sensitive information. From an oversight perspective, monitoring the development by Swift of post-quantum cryptography capabilities fits in with the objectives of long-term security planning and data confidentiality, thereby helping to future proof the environment in which Swift operates and ultimately ensure trust in the global financial industry.

Another topic of interest to overseers is third-party risk management (TPRM), sometimes referred to as "supply chain risk management" or "vendor risk management". Reliance by financial institutions on third parties, such as technology providers and service contractors, introduces significant operational, regulatory and reputational risks. These third parties often have access to sensitive financial data and systems, making them potential points of vulnerability for cybersecurity threats, data breaches or service disruptions. To gain assurance that Swift is adequately managing and mitigating such risks, TPRM was covered in depth by way of an on-site review in 2023, which resulted in a number of recommendations. Swift proposed a set of actions to address these recommendations, the implementation of which is being followed up on by the overseers.

Physical security is critical to an organisation's overall security posture and, in combination with cybersecurity, 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.

To gain additional assurance that Swift is meeting the oversight expectations in terms of cyber and physical security, overseers organise on-site visits to its premises. 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. See Box 7 for more information on the on-site review of change management carried out in 2024.

BOX 7

On-site review of change management in 2024

For the past few years, overseers have conducted an annual on-site review (OSR) to allow a comprehensive assessment of specific topics for which they seek additional insight or assurance. The OSR kicks off with an extensive document review, to gain knowledge of the subject at hand. This is followed by a week at Swift's headquarters, during which time the OSR team attends presentations on the subject matter, interviews relevant staff, and participates in walkthroughs showcasing real-life practices.

The OSR has proven to be an effective means of gaining a deeper understanding of selected topics. It enables overseers to provide well-informed recommendations, thereby enhancing the maturity of relevant practices, policies and procedures at Swift. OSRs are conducted by a multidisciplinary team comprising representatives from multiple central bank members of the cooperative oversight arrangement.

In 2024, the Swift Oversight Group (OG) decided to conduct an OSR on the topic of change management, to examine Swift's change management practices, policies and procedures and assess whether they adequately meet oversight expectations. In order to maximise the value of the OSR and gain a comprehensive understanding of how change is managed at Swift, the overseers decided to include release and deployment management in the scope of the review. These terms are defined as follows:

- Change management: Change management ensures that modifications to IT systems and processes are systematically planned, evaluated, and implemented with minimal risk to business operations.
- Release management: Release management oversees the bundling, testing and scheduling of updates or new features to ensure the smooth delivery and functionality of IT services.
- Deployment management: Deployment management handles the physical rollout and installation of software or hardware changes into the live environment while minimising disruptions.

From an oversight perspective, the adequate functioning of these processes is critical, as they directly impact the reliability, security and resilience of the systems underpinning Swift's products and services for the global financial sector. Effective change management practices ensure that updates and modifications are thoroughly assessed and implemented without introducing new vulnerabilities. Release and deployment management are crucial for maintaining operational continuity, as poorly executed changes can lead to system outages and data integrity issues, which may have a cascading effect on other actors in the financial ecosystem.

Following the OSR and based on the documentary evidence and learnings from interaction with Swift staff, the OSR team formulated a number of observations regarding possible improvements. These observations were set out in a report which was approved by the OG and provided to Swift. The resulting actions to address these observations will be followed up on in 2025.

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. Under the CSP, users are required to adhere to certain controls and good practices to secure appropriately their on-site ICT environment 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.

Since the introduction of the CSP, Swift has taken multiple initiatives to improve various of its aspects, such as an annual review of the Customer Security Control Framework (CSCF), improvements to the Know-Your-Customer Security Attestation (KYC-SA) application, the launch of an Independent Assessment Framework (IAF), the introduction of compulsory assessments, more effective involvement on the part 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 expects to continue to enhance it.

One such initiative concerns the involvement of supervisory authorities in the use of CSCF security 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-Customer for Supervisors (KYS) application have proven challenging as, in some cases, multiple supervisory authorities are responsible for a single country. 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, the overseers contributed, together with the National Member Groups, to the yearly review of the Customer Security Control Framework (CSCFv2025). This review did not result in new mandatory controls, but clarifications were made to facilitate users' ability to comply with the individual control objectives. In addition, some controls benefit from a phased approach whereby in-scope components are defined so as to allow users to start identifying which components in their environments may become subject to mandatory controls in the future.

Swift users are expected to comply with mandatory security controls (i.e. the security baseline) and can attest to their compliance with advisory controls (i.e. good practices for securing local IT infrastructure). Self-attestations must be uploaded using the Know-Your-Customer Self-Attestation (KYC-SA) application by the end of each year. A new version of the CSCF was introduced in mid-2024, and users have until the end of 2025 to submit their attestations.

By 31 December 2024, 83% of Swift customers had submitted a valid attestation for compliance with the CSCF; of these self-attestations, 82% of customers indicated compliance with all mandatory controls. Compliance levels and the number of self-attestations were in line with the uptake in 2022 and 2023. Through Swift's quality assurance reports and monthly metrics reports, overseers closely monitor various CSP-related metrics, 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. For this reason, the overseers expect Swift to refine and extend the CSP reporting metrics as appropriate.

The Independent Assessment Framework (IAF), 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 has to subject their attestations to either an independent internal assessment (for example, by the second or third line of defence) or an independent external assessment (by a consultancy firm, for example). Users are free to select the internal and/or external resources used to conduct the assessment. If a user opts for self-attestation without an independent internal or external assessment, it will be considered non-compliant with the CSP.

Initial reporting on compliance with the IAF was in keeping with previous years, with 91% of users opting for an independent assessment and thus remaining in line with CSP requirements. Of these users, about half opted for an independent internal assessment and half for an independent external assessment. The percentage of Swift traffic sent by customers with IAF-compliant attestations remained constant, at around 99%.

Introduced at the end of 2023, the Swift Customer Security Programme Assessor Certification (CSPAC) is a relatively new addition to the CSP. Swift launched this programme to address certain challenges faced by the community in adhering to the IAF, such as scope creep and cost overrun, primarily due to gaps in the standardisation of deliverables and inconsistency in the quality of assessor activities as well as in response to customer requests for a list of trusted certified assessors. The objective of the CSPAC programme is 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 and Transaction Manager

ISO 20022 is an open global standard for the transfer of financial messages and information. It provides consistent, rich and structured data which can be used for all types of financial transactions. The global migration of Swift to this new format, which began in 2023, is taking place in phases, with a coexistence period during which both traditional Swift MT messages and ISO 20022 (MX) messages are supported. The coexistence period is set to end on 22 November 2025, after which time ISO 20022 will become the sole standard for cross-border payments and reporting.

At the end of 2024, ISO 20022 messaging was being used for over 32% of the total volume of cross-border payments and reporting traffic (CBPR+), as measured since the start of the coexistence period. In addition, around 30% of payment market infrastructures (PMIs) had migrated to the new standard, representing over 73% of global PMI traffic volume.

As a global standard setter, Swift is coordinating the migration to ISO 20022 for its community. From the start, overseers have closely monitored Swift's approach, project management and planning, risk assessment, and communication with users. As the co-existence period for the concomitant use of Swift MT and

ISO 20022 messaging for CBPR+ traffic will come to an end in November 2025, it is critical that the global customer base be migrated to ISO 20022 messaging by that date. To this end, the overseers will continue to follow up on Swift's initiatives and communication efforts to facilitate the timely migration of users to the new standard prior to expiry of the coexistence period.

Swift's Transaction Management Platform (TMP) is closely related to ISO 20022. In 2019, Swift revealed plans to develop the TMP in a push to move away from traditional sequential messaging to a platform that allows every participant in a transaction to have an end-to-end and up-to-date view of its status.

By shifting from secure message forwarding to end-to-end transaction management through the TMP, Swift aims to rely on richer data and reduce friction (i.e. provide a better customer experience, improve efficiency, and offer new value-added services such as transaction validation). The underlying communication channel for the transaction is format agnostic and can be FIN MT, ISO 20022 MX, or a combination of channels depending on the capabilities of the parties involved (i.e. backward compatibility). The platform ensures that full transaction data are available to any authorised party in the transaction chain, thus allowing end-to-end transparency. In the future, the TMP may be used to facilitate the use of application programming interfaces (APIs) so that authorised users can retrieve their transaction status via an API call over the Swift network.

Transaction Manager went live in November 2022 and began 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 the tool.

4.2.4 Swift's contribution to the G20 Roadmap for Enhancing Cross-border Payments

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

One example is the aforementioned industry-wide migration to ISO 20022, which is scheduled to be completed in November 2025. This will set the stage for a new level of operational efficiency and innovation. The adoption of a common messaging format, such as ISO 20022, can 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.

Swift is contributing to the G20 initiative by rolling out various value-added services which financial institutions can use to eliminate friction and overcome the existing challenges in cross border payments. In September 2023, Swift announced that it would introduce Swift Essentials, a portfolio of value-added services, including GPI, Swift Go, Payment Pre-validation, Transaction Screening (TSS), and Payment Controls (PCS). Since 1 January 2024, Swift Essentials has been available to all Swift users, which can choose the components or value-added services they wish to use and receive a single annual invoice for in-scope services.

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.

Another way in which Swift supports the G20 roadmap is its Global Payments Innovation (GPI) initiative. Launched in 2017, this programme is considered the new standard for large-value cross-border payments. Swift GPI combines traditional Swift messaging and banking services with a new set of rules. Any financial institution joining GPI has to abide by these rules, which govern the transparency of fees, end-to-end payment tracking, and confirmation of credit to the recipient's account.

The benefits of joining GPI are numerous. First, GPI substantially increases payment speed. It eliminates friction and reduces the risk of delays through upfront account verification. Another way GPI reduces friction is through automated exception management processes, allowing users to easily handle queries between banks in the Swift network and resolve instances of incorrect or missing payment information. Another important aspect, for cross-border transactions, is financial crime compliance. GPI offers a portfolio of financial crime compliance solutions to help member institutions navigate more complex compliance requirements.

Whereas Swift GPI is used for high-value or wholesale cross-border payments, Swift Go aims to facilitate 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 in order to offer their customers an easy and intuitive payment experience. In this way, Swift aims to ensure that the traditional banking sector remains competitive in the high-growth market for low-value cross-border payments.

The services and products outlined above illustrate Swift's eagerness to support the industry's push towards 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.

4.3 Focal points for Swift oversight in 2025

The annual planning of Swift oversight is driven by a risk-based approach. An oversight risk assessment is performed to maximise the effectiveness and efficiency of the planned activities. After each quarter, overseers evaluate the topics analysed and decide which require deeper review or the areas in which Swift needs to provide more information. This approach allows oversees to spend more time on specific topics, where appropriate, and to coordinate follow-up discussions at a later stage.

Swift operates in a fast-paced environment characterised by increasing competition and rapidly evolving technologies. This context affects its go-to-market strategy (e.g. new product offerings and an evolution towards agile software development) and operations (e.g. the software development life cycle, incident management and business continuity). Furthermore, Swift is expected to manage a range of emerging challenges, such as geopolitics, the global scarcity of skilled resources and the changing cyber threat landscape. Overseers consider this changing environment and continuously monitor how it affects Swift in terms of technology planning, resilience guarantees, risk assessments, security decisions, and design choices. Overseers seek assurance at all times that the risks arising from new technological choices and major projects are adequately identified, managed and mitigated, to ensure business continuity with comparable or better resilience.

Cybersecurity strategy and cyber risk management remain important topics on the oversight agenda for 2025. Overseers analyse Swift's proposed security and IT investments and assess how enhanced capabilities will help protect it against increasingly sophisticated cyberattacks. The cybersecurity review also involves challenging the ISAE 3000 reports prepared by Swift's external security auditor. These reports provide independent assurance on Swift's internal policies, procedures and controls for each of the five HLEs. They contain rich information important for the oversight of Swift and are thoroughly reviewed each year.

The software development lifecycle (SDLC) is intricately connected to both organisational security and operational resilience. Throughout the SDLC, security measures can be integrated to identify and address vulnerabilities, ensuring that the customer-facing product offerings developed by Swift can withstand potential threats.

By incorporating security considerations, including requirements and design, at an early stage, organisations can proactively mitigate risks and enhance the overall security posture of their systems.

Another closely related topic is change management. Change management processes are intended to control and manage alterations to the IT environment, which is essential in order to maintain a secure and stable infrastructure. As outlined in Box 7, change management was the focus of the 2024 on-site review. Key aspects of Swift's SDLC were covered as well. In 2025, overseers will continue to follow up on the actions taken by Swift to address the recommendations resulting from the OSR.

Due to a recent uptick in service availability-related issues, overseers will continue to monitor and refine Swift's policies and processes for problem and incident reporting. As lead overseer, the Bank is the central point of contact for Swift-related incidents and is well positioned to engage with other supervisors or central banks to discuss issues liable to impact institutions under their jurisdiction. The clear and correct reporting of information during incidents helps mitigate the risk of information asymmetries within the financial community, thereby leading to smoother and faster remediation of issues.

CSP follow-up also forms part of the oversight activities planned for 2025. In particular, the Swift user community's level of compliance with CSCF controls, developments concerning customer cases, the results of the new independent assessment requirement, and the CSPAC are of interest to overseers. The Bank, in its capacity as lead overseer, will use the in-person meeting of the Swift Oversight Forum to provide an update on the proposed changes to the CSCF. The aim is to encourage other national authorities to continue to push the institutions under their supervision to improve endpoint security and for authorities and supervisors to leverage the capabilities of the know-your-supervisor self-assessment data in their oversight toolbox.

Oversight planning is structured around the five HLEs, which form the starting point for the selection of topics for review. In accordance with a risk-based approach, the previous year's assessment is used to plan activities for the coming year. For 2025, this resulted in an extensive set of topics to be analysed by overseers, the most important of which are listed below:

- HLE 1 - Risk Identification and management.
  - Swift's overall risk profile and topic-specific risk assessments.
  - Implementation 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 post-quantum cryptography roadmap.
  - Cybersecurity controls, in particular preventive and detective controls.
  - Thread-led penetration testing (red teaming) at Swift.
- HLE 3 - Reliability and resilience.
  - Incident management and business continuity.
  - Implementation of action items resulting from the OSR of change management.
- HLE 4 - Technology planning.
  - IT technology roadmap and drivers for investment.
  - Investment in Swift's layered resilience.
  - New product and service offerings.
- HLE 5 - Communication with users.
  - Continuing engagement with the global user community.
  - Communication to users on specific topics such as the migration to ISO 20022 by November 2025 and the yearly CSP attestation cycle.
  - Appropriate collaboration with the global userbase to enhance the resilience of end-users.