4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium that provides messaging services to both financial institutions and market infrastructures. These customer types are characterized by their diversity in terms of activities and size, e.g. SWIFT serves banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparties and trusts.

Nearly half of SWIFT messaging activity is related to the exchange of payment information between banks involved in correspondent banking arrangements. SWIFT provides messaging and connectivity services to a large number of market infrastructures, e.g. in the context of large-value payment systems (section 3.1) to help limit settlement risks in the interbank payment process. Messaging services are also being provided to CLS Bank (see box 6) that eliminates settlement risk for foreign exchange transactions between currencies.

Additionally, the cooperative is an active promotor of structural cooperation within the payment and settlement industry. In collaboration with its members, SWIFT focuses on refining existing message types and defining message standards for new transaction types or other financial information needs. Recently, SWIFT has also been focusing on improving the cyber resilience of its customers by supporting them in securing their local infrastructure.

Although SWIFT is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily messaging, so that SWIFT – as a critical service provider (CSP) to these systems – is itself of systemic importance (see chart 18 below). For these reasons, the central banks agreed to make SWIFT subject to cooperative central bank oversight (see box 9). By jointly interacting with SWIFT and formulating joint recommendations vis-à-vis SWIFT, central banks aim to increase the efficiency of their interactions with SWIFT as well as the effectiveness of the SWIFT actions taken in reaction to their recommendations.

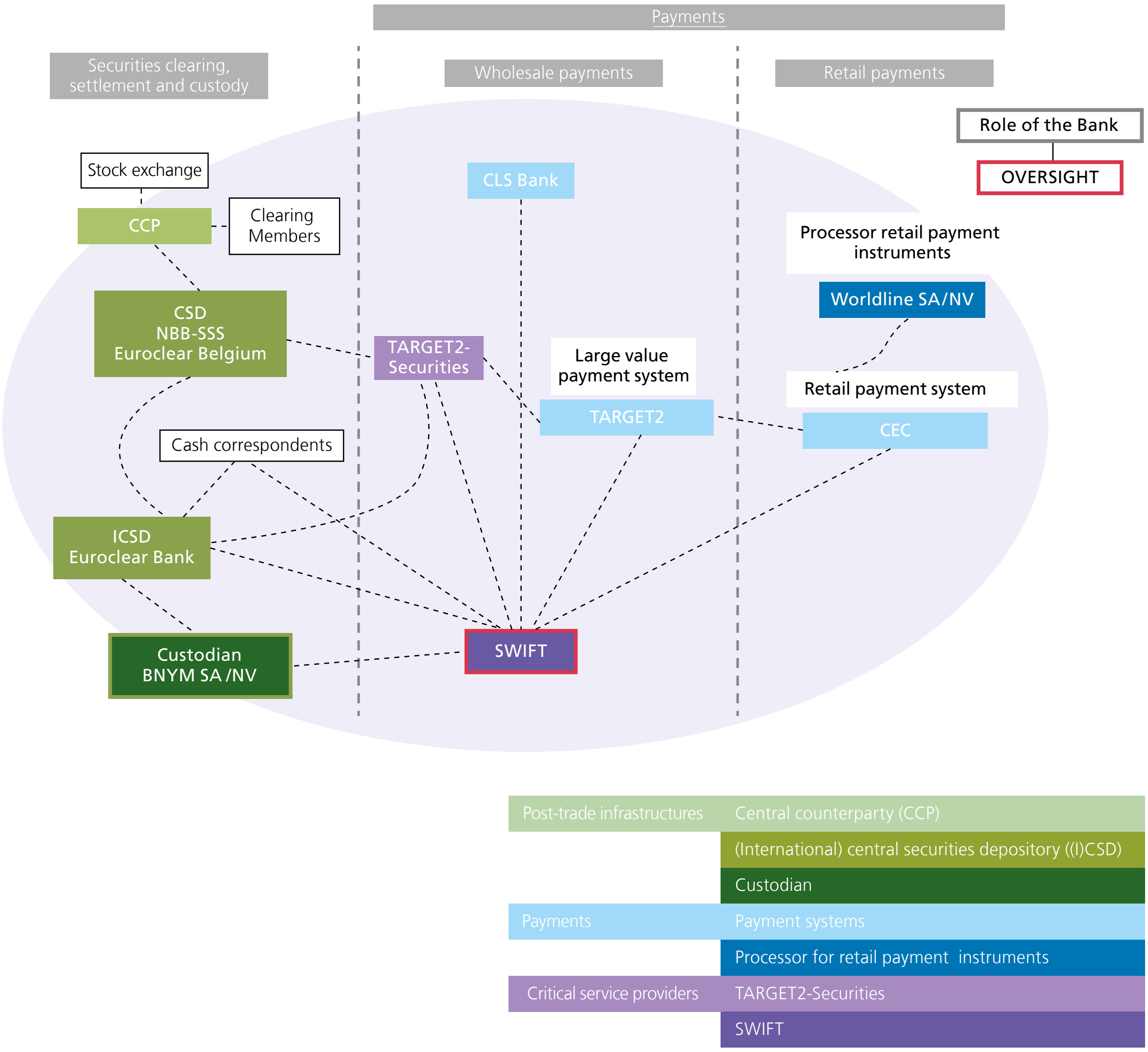
SPECIFIC ATTENTION POINTS IN THE OVERSIGHT FRAMEWORK

While the regulatory framework for SWIFT remains unchanged, the overseers have identified the Customer Security Programme as an important area within scope of the oversight arrangement. The development and roll-out of this programme exposes both SWIFT and its customers to specific risks, while at the same time a successful adherence to the Customer Security Programme by SWIFT's participants would increase overall cyber resilience.

Recent cyber incidents at SWIFT participants have indicated the importance of effective cyber security measures at all entities involved in the processing of financial transactions, i.e. end-to-end security in the transaction chain. SWIFT informed the overseers and its customers of these cyber incidents and indicated it obtained reasonable assurance that neither the network nor the operations had been compromised. As attackers were able to exploit weaknesses in the IT environment of SWIFT's customers, a need for reiterating the importance of end-to-end security in the transaction chain was identified.

SWIFT's Customer Security Programme is dedicated to support its customers in reinforcing the cyber security measures of their SWIFT infrastructure and adds an important security framework for other financial institutions and market

CHART 18 SWIFT AS CSP TO THE FINANCIAL INDUSTRY AND THE BANK'S OVERSIGHT ROLE


Payments
Securities clearing, settlement and custody
Wholesale payments
Retail payments
Role of the Bank
OVERSIGHT
Stock exchange
CCP
Clearing Members
CLS Bank
Processor retail payment instruments
Worldline SA/NV
CSD NBB-SSS Euroclear Belgium
TARGET2-Securities
Large value payment system
Retail payment system
TARGET2
CEC
Cash correspondents
ICSD Euroclear Bank
Custodian BNYM SA /NV
SWIFT
Post-trade infrastructures
Central counterparty (CCP)
(International) central securities depository ((I)CSD)
Custodian
Payments
Payment systems
Processor for retail payment instruments
Critical service providers
TARGET2-Securities
SWIFT

infrastructures. It is designed around three mutually reinforcing areas: secure and protect; prevent and detect; and share and prepare.

The first area, secure and protect, focuses on improving the cyber security posture of SWIFT's customers. A core set of mandatory security controls that aim at enhancing the security baselines is provided. Customers will be asked to attest their compliance. Given the potential impact on the financial industry, the overseers continue to review and assess the effectiveness of the proposed measures. Similarly, the strengthening of the security requirements for customer-managed software is being followed up.

The second area, prevent and detect, deals with the development and promotion of detection mechanisms at the message sender's side, as well as the active management of counterparty relationships (e.g. ensuring that you can only receive messages from trusted parties). These applications fall in the traditional oversight scope.

The third area, share and prepare, centres on deepening SWIFT's cyber security forensics and analysis capabilities so as to develop intelligence on SWIFT-related events.

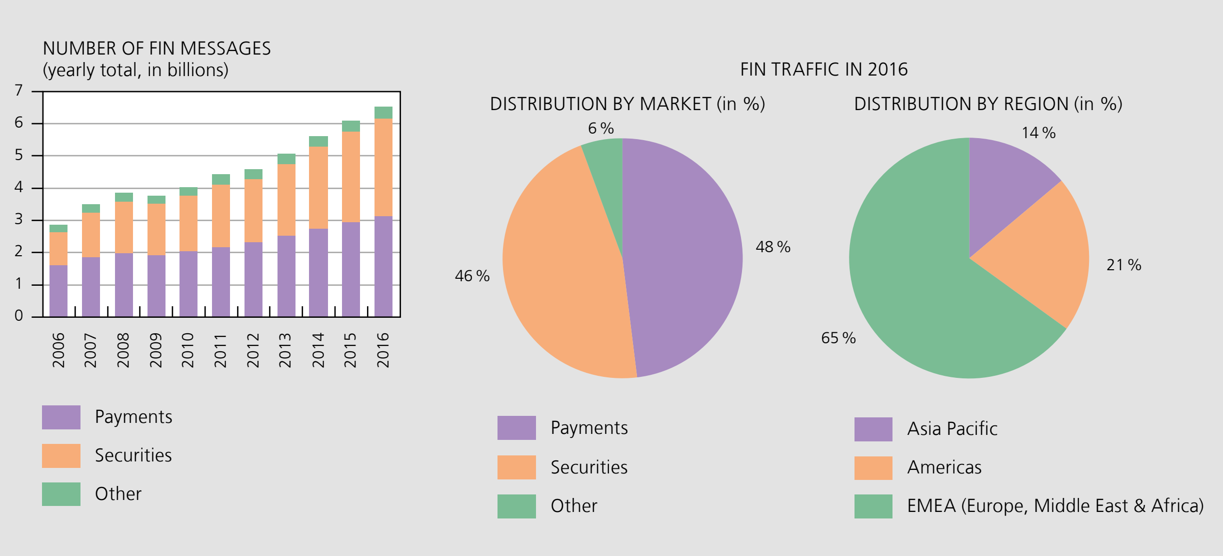
In June 2016, the NBB issued on its website a joint statement of the SWIFT overseers on reinforcing cyber resilience of the financial ecosystem[1]. The document expresses the common understanding of the importance of the cyber security arrangements of SWIFT's users in the overall cyber resilience of the financial system.

BUSINESS ACTIVITY

SWIFT is owned and controlled by its members. It has an ongoing dialogue with its users through national member groups, user groups and dedicated working groups. These discussions relate, for example, to SWIFT's activities such as proposals for new or revised standards, providing industry comments on proposed corporate or business service changes, and comments on timeframes for new technology or service implementation. Each member has a number of shares proportional to its usage of SWIFT's message transmission services. Every three years, a share reallocation is implemented to reflect changes in each member's use of SWIFT. Countries or country constituencies can recommend directors to the board according to the number of shares owned by all members in each country.

FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2016 reached 6.5 billion messages (+ 6.5 % compared to previous year), i.e. about 25.8 million messages per day. While large-value payment systems have contributed significantly to the growth in messaging via SWIFT in the previous decade, the growth in securities traffic has been even greater: securities messaging grew from one-third of SWIFT's total traffic to nearly half of the traffic (chart 19, left panel). These messages flow between participants in stock exchanges, payment systems, (I)CSDs and CCPs, as depicted in chart 18. SWIFT FIN traffic in 2016 was about 48 % related to payments and 46 % to securities messaging, while the main part of the traffic originated from EMEA members (65 %), before those from the Americas region (21 %) (chart 19, right panel).

CHART 19 SWIFT FIN ACTIVITY



Source: SWIFT.

OVERSIGHT APPROACH

SWIFT's messaging activities for payment and securities settlement infrastructures has been recognised as a significant factor in the safety and efficiency of payment and securities settlement systems. The Bank acts as the lead overseer – SWIFT is incorporated in Belgium – and conducts the oversight in direct cooperation with the other G10 central banks.

[1] https://www.nbb.be/doc/cp/eng/publications/swiftoversightforum.pdf.

In 2012, the arrangement was complemented with a structure comprising the senior overseers form the G20 countries, which discusses oversight policy and results. A complete overview of the oversight set-up can be found in box 9.

Box 9 – The international cooperative oversight of SWIFT

As lead overseer, the Bank conducts the oversight of SWIFT in cooperation with the other G10 central banks (i.e. Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System).

The Bank monitors SWIFT developments on an ongoing basis. It identifies relevant issues through the analysis of documents provided by SWIFT and through discussions with the management. It maintains a continuous relationship with SWIFT, with regular ad hoc meetings, and serves as the G10 central banks' entry point for the cooperative oversight of SWIFT. In that capacity, the Bank chairs the senior policy and technical groups that facilitate the cooperative oversight, provides the secretariat and monitors the follow-up of the decisions taken.

The various SWIFT oversight groups are structured as follows:

- the SWIFT Cooperative Oversight Group (OG), composed of all G10 central banks, the ECB and the chairman of the CPMI, is the forum through which central banks conduct cooperative oversight of SWIFT, and in particular discuss oversight strategy and policies related to SWIFT.
- within the OG, the Executive Group (EG) holds discussions with SWIFT's Board and management on the central banks' oversight policy, issues of concern, SWIFT's strategy regarding oversight objectives, and the conclusions. The EG supports the Bank in preparing for discussions within the broader OG, and represents the OG in discussions with SWIFT. The EG can communicate recommendations to SWIFT on behalf of the OG. At one of the EG meetings, the annual reporting by SWIFT's external security auditor is discussed. The EG includes the Bank of Japan, the Federal Reserve Board, the Bank of England, the ECB and the Bank;
- at the technical level, the SWIFT Technical Oversight Group (TG) meets with SWIFT management, internal audit and staff to carry out the groundwork of the oversight. Specialised knowledge is needed to understand SWIFT's use of computer technology and the associated risks. The TG draws its expertise from the pool of staff available at the cooperating central banks. It reports its findings and recommendations to the OG.

The SWIFT Oversight Forum is composed of senior overseers from the G10 central banks (OG) and 10 additional central banks (i.e. Reserve Bank of Australia, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Korea, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank and Central Bank of the Republic of Turkey). Its objectives are to:

- facilitate a coordinated flow of information about SWIFT oversight conclusions to the Forum participants;
- foster discussions on the oversight policy concerning SWIFT;
- provide input to the OG on priorities in the oversight of SWIFT;
- serve as a communications platform on system interdependencies related to the common use of SWIFT or for communication in case of major contingency situations related to SWIFT.

The overseers' focus on SWIFT's management of operational risks is articulated into five High Level Expectations (HLEs) that focus on risk management (see box 10). These HLEs are providing SWIFT and overseers with a common language, a framework within which discussions can be held. These expectations vis-à-vis SWIFT have evolved into generic oversight requirements for all critical service providers to FMIs and were included as Annex F in the CPMI-IOSCO Principles for FMIs[1].

[1] CPMI-IOSCO (2012), Principles for financial market infrastructures, BIS (http://www.bis.org/publ/cpss101a.pdf).

SWIFT provides the overseers with a regular self-assessment report regarding its compliance with the HLEs. This compliance assessment does not reflect the overseers' opinion, but is one of the starting points for the identification and further analysis of risk drivers at SWIFT.

Cyber and information security, a major driver for operational risk at SWIFT, has been a standing topic in the oversight of SWIFT. Based on cyber threat and strategy discussions with the security experts of SWIFT, the overseers conduct a risk assessment and identify the review priorities. In 2016, the overseers focused on the processes for cyber event detection, monitoring and response, taking also into account the use and creation of cyber intelligence at SWIFT. The interaction with and communication strategies for international Information Sharing and Analysis Centres (ISACs) has been analysed. Yearly, the overseers also review the processes for business continuity and disaster recovery.

The results of logical intrusion tests (with a specific testing scope such as one particular system or interface) and red team tests (i.e. expert team that is not bound by a testing scope) are extensively reviewed by the overseers and discussed with the management and security experts, and the remediation plans are reviewed. Overseers also followed up on the scale-up of the red teams and the available security skill mix. Deep-dives have been conducted towards the processes for assessing, managing and patching vulnerabilities, as well as the interaction with third-party vendors. Yearly, the overseers have the opportunity to challenge the external security auditor and its findings.

Overseers are also seeking to obtain reasonable assurance that entry points to the SWIFT network that are beyond its control are well-managed. Due diligence criteria and assessments for consumers, shared infrastructure providers and vendors of interface software are being monitored. In this context, the overseers have identified the Customer Security Programme that reaches well beyond SWIFT as a long-term area of oversight attention.

Additionally, SWIFT regularly presents its long-term technology strategic thinking and concrete platform investments. Major projects include cyber security investments, technological renewals and projects to improve efficiency and effectiveness for the customers such as the Global Payment Innovation Initiative[1]. The strategic proposals are challenged and tested against the overseers' requirements for security with special attention for information confidentiality, integrity and availability.

Overseers conduct regular evaluations of the effectiveness of the different lines of defence and governance structures, for daily operations, long-term strategies and specific projects (e.g. Customer Security Programme). Specific attention goes to the development and implementation of the enterprise risk management roadmap and the recurring assessment of extreme risks and recovery plans.

When incidents take place in SWIFT's infrastructure, network or operations, the overseers investigate the sequence of the events, analyse the customer impact and review results of the investigation. Detailed preventive action plans that outline the activities, deadlines and responsibilities within SWIFT are requested where necessary. Frequent follow-up on these preventive action plans is being conducted.

[1] https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi.

Box 10 – High Level Expectations (HLEs) for (the oversight of) SWIFT

HLE 1. RISK IDENTIFICATION AND MANAGEMENT

SWIFT IS EXPECTED TO IDENTIFY AND MANAGE RELEVANT OPERATIONAL AND FINANCIAL RISKS TO ITS CRITICAL SERVICES AND ENSURE THAT ITS RISK MANAGEMENT PROCESSES ARE EFFECTIVE.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

- the processes for risk identification and management, documenting the identified risks, the controls implemented to manage those risks, and the decisions made to accept risks;
- the processes for reviewing previously accepted risks in the light of new information;
- SWIFT's structures and processes set up to manage risks effectively;
- the extent to which SWIFT provides for effective assessments of risks and risk management processes through board of directors' oversight and independent internal and external audits.
- the extent to which the internal audit:
    - adheres to the principles of a professional organisation, such as the Institute of Internal Auditors, which govern audit practice and behaviour;
    - independently assesses inherent risks, as well as the design and effectiveness of risk management processes and internal controls to mitigate risks; and
    - clearly communicates its assessments to relevant Board members and has direct and immediate access to the chair of the Board's Audit & Finance Committee.
- how risks are monitored and managed in various domains, including at least the following:
    - dependency on third parties;
    - legal and regulatory requirements pertaining to SWIFT's corporate organisation and conduct;
    - relationships with customers;
    - strategic decisions with an impact on the longer-term continuity of the critical services;
    - risks related to information security, reliability and resilience, and technology planning, which are further elaborated on in HLEs 2, 3 and 4.

HLE 2. INFORMATION SECURITY

SWIFT IS EXPECTED TO IMPLEMENT APPROPRIATE POLICIES AND PROCEDURES, AND DEVOTE SUFFICIENT RESOURCES, TO ENSURE THE CONFIDENTIALITY AND INTEGRITY OF INFORMATION AND THE AVAILABILITY OF ITS CRITICAL SERVICES.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

- information security policy or framework, and any processes and procedures for monitoring compliance;
- capacity planning;
- change management practices; and
- assessments of the implications of changes to SWIFT's operations on information security.

HLE 3. RELIABILITY AND RESILIENCE

COMMENSURATE WITH ITS ROLE IN THE GLOBAL FINANCIAL SYSTEM, SWIFT IS EXPECTED TO IMPLEMENT APPROPRIATE POLICIES AND PROCEDURES, AND DEVOTE SUFFICIENT RESOURCES, TO ENSURE THAT ITS CRITICAL SERVICES ARE AVAILABLE, RELIABLE AND RESILIENT AND THAT BUSINESS CONTINUITY MANAGEMENT AND DISASTER RECOVERY PLANS SUPPORT THE TIMELY RESUMPTION OF ITS CRITICAL SERVICES IN THE EVENT OF AN OUTAGE.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

- business continuity and disaster recovery objectives, strategies and plans, including the extent to which they address the risk of a major operational disruption;
- business continuity and disaster-testing plans, procedures, and results, including the extent to which SWIFT facilitates periodic testing with customers; and
- procedures and processes to record, report, and analyse all operational incidents.

▶

HLE 4. TECHNOLOGY PLANNING

SWIFT IS EXPECTED TO HAVE IN PLACE ROBUST METHODS TO PLAN FOR THE ENTIRE LIFECYCLE OF THE USE OF TECHNOLOGIES AND THE SELECTION OF TECHNOLOGICAL STANDARDS.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following :

- IT strategic plans and processes for maintaining and updating those plans ;
- the extent to which technology decisions balance the near-term needs of individual service enhancements with the planned long-term technology path for the service ;
- assessments of the maturity of technologies being evaluated for introduction into the SWIFT environment ;
- standards selection process when deploying and managing a service, and the standards maintenance and review process over time ; and
- processes to ensure that design choices consider information security risks for the user community.

HLE 5. COMMUNICATION WITH USERS

SWIFT IS EXPECTED TO BE TRANSPARENT TO ITS USERS AND PROVIDE THEM INFORMATION THAT IS SUFFICIENT TO ENABLE USERS TO UNDERSTAND WELL THEIR ROLE AND RESPONSIBILITIES IN MANAGING RISKS RELATED TO THEIR USE OF SWIFT.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following :

- customer communication procedures and processes to inform users of :
    - their role and responsibilities, including in the case of disruptions to SWIFT's critical services (crisis communication) ;
    - SWIFT's management processes, controls, and independent reviews of the effectiveness of these processes and controls ; and
    - identified weaknesses (absent or non-performing controls) if users need such information to manage risks related to their use of SWIFT ;
- techniques SWIFT uses to be informed by users of operational risks on the user side that could potentially affect its own operations, or, alternatively, techniques SWIFT uses to prevent any such user impact on its operations ; and
- consultative mechanisms to ensure that SWIFT's technology choices that affect user operations are acceptable to the principal users of the critical services.

OVERSIGHT PRIORITIES IN 2017

The primary oversight focus for 2017 is on the adequacy of SWIFT's cyber strategy for the infrastructure, network and operations under its responsibility. In addition to a review of the investments in cyber security measures, a series of in-depth reviews are foreseen such as the hardening of the SWIFT tools, the identity and access management measures and the security culture.

In line with the need for a more holistic approach to cyber security, the overseers will continue to follow-up on the roll-out of SWIFT's Customer Security Programme. Part of this follow-up will be an assessment of the adequacy of the mandatory security controls and the transparency of communications with users on cyber security events and responsibilities.

Additionally, the overseers have a selection of standing topics. Firstly, the overseers continuously assess the effectiveness of the three lines of defence, i.e. line management, risk management and internal audit. Targeted oversight analyses should provide insight in the strategic infrastructure decisions, as well as the functioning of the enterprise risk management processes (e.g. risk identification, documentation and management). A selection of internal audit reports will be reviewed to obtain reasonable assurance on the independence and objectivity of the internal auditor. Objective and independent audits provide the overseers with important evidence on the risk mitigation capabilities and security posture of SWIFT. Additionally, the findings, if any, of the external security auditor will be analysed and potential remediation discussed.

Secondly, the overseers start from the analysis of the risk of major operational disruption, to analyse and evaluate the business continuity processes, disaster recovery objectives and strategies. In this context, the overseers will assess the processes and strategies against the requirements elaborated in the new CPMI-IOSCO guidance on cyber resilience[1]. Special attention will go to the proposals for the 2 hour recovery time objective specified in the guidance.

Thirdly, risk-based assessments for strategic IT decisions and technology renewal are being conducted, as well as a review of the vendor due diligence processes and incident response integration. These risk assessments explicitly take into account the implications for the confidentiality, integrity and availability of information for the infrastructure, network and operations under control of SWIFT and of its users.

Fourthly, the overseers will judge the communication procedures and processes to inform users of their roles and responsibilities. In the light of the recent cyber incidents and the importance of the distribution of actionable cyber threat intelligence, the overseers decided to analyse the procedures and processes for communicating weaknesses identified at SWIFT or one of its customers to SWIFT's community.

Finally, the overseers continue to analyse the design and follow-up on the implementation of major projects that could significantly impact the risk profile of SWIFT. Overseers will seek assurance that SWIFT has sufficient attention for the security features of its interfaces when further developing them in line with the evolving cyber threat evolutions. Additionally, the overseers will focus on the security requirements (and their differentiation) for the different options to access SWIFT services, this includes an analysis of the due diligence criteria, processes and results for third-party interfaces and shared infrastructure providers.

[1] CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, BIS (http://www.bis.org/cpmi/publ/d146.pdf).