High level expectations for the oversight of SWIFT

Introduction

S.W.I.F.T. s.c.r.l. ("SWIFT"), the Society for Worldwide Interbank Financial Telecommunication, was set up in 1973 with the specific objective to serve the cross-border, international financial markets with messaging services for correspondent banking. The volume of payments messages processed by SWIFT has grown enormously since the inception of the infrastructure, partly because SWIFT started offering services in a growing number of areas in the financial sector. Besides its support for correspondent banking activities, SWIFT now also processes messages for the securities industry (settlement, corporate actions, reporting,…) or messages related to treasury operations and to international trade finance. Since the early nineties, SWIFT has thus become a key messaging provider for payment and securities settlement infrastructures throughout the world. SWIFT currently offers services to 83 large value payment systems (primarily Real Time Gross Settlement systems operated by central banks) and also processes messages for CLS, the infrastructure that enables payment versus payment settlement of foreign exchange transactions.

Central banks have long recognised the paramount importance of a smoothly functioning payment and settlement infrastructure, both for the effective implementation of monetary policy and for the efficiency and stability of the financial system in general. Central banks monitor SWIFT closely because of its critical role for the functioning of those infrastructures.

Until 1998, central bank interaction with SWIFT to discuss the stable functioning of SWIFT mainly consisted of a few high-level meetings a year. As from 1998, the central bank interaction with SWIFT was placed on a more formal footing with the initiation of central bank "oversight" of SWIFT. Oversight is defined as a public policy activity principally intended to promote the safety and efficiency of payment and securities settlement systems and in particular to reduce systemic risk. Since 1998, the practical SWIFT oversight arrangements have gradually evolved. Since then, the central bank focus on a stable and robust financial infrastructure increased further, and the SWIFT oversight activity intensified. The most recent review of the SWIFT oversight arrangements took place in 2004. The review led to a strengthening of the practical arrangements, which are described in the NBB's 2005 FSR issue. In short, the oversight of SWIFT is performed by the NBB as lead overseer in cooperation with the G10 central banks. The NBB is the lead overseer of SWIFT, for SWIFT is a company governed by Belgian law and has its head offices in Belgium. There is a protocol arrangement between the NBB and SWIFT on the objectives of the SWIFT oversight, and the NBB also concluded bilateral Memoranda of Understanding with each of the other central banks participating in the oversight of SWIFT.

This article presents the "High Level Expectations for the Oversight of SWIFT" that have been recently developed by the overseers of SWIFT. The first section explains why overseers thought it appropriate to develop specific High Level Expectations for SWIFT. The second one presents each of the 5 High Level Expectations and highlights their scope of application. The third section explains how the HLEs will be used. The full text of the HLEs as shared by the overseers with SWIFT are added for reference in the annex to this article.

1. Rationale for defining High Level Expectations for the Oversight of SWIFT

In recent years, in order to structure their oversight activities, central banks have devoted considerable efforts to setting up standards, principles or recommendations for the effective oversight of systemically important payment systems, securities settlement systems and central counterparties[1]. Such standards not only serve the central banks for their oversight activities, but also give the overseen systems/infrastructures an indication of what they are expected to comply with. To facilitate their implementation and enforcement, overseers also seek to set out clear and comprehensive methodologies for the use of the recommendations in assessments, be it in self-assessments by the systems themselves, assessments by overseers or peer reviews of such self-assessments.

The SWIFT Cooperative Oversight Group (OG) reviewed whether it could apply the Core Principles for Systemically Important Payment Systems as a framework for its oversight of SWIFT, but the Group concluded that that would not be appropriate. Indeed, SWIFT is not itself a payment system, but a messaging services provider to such systems, so that many of the Core Principles do not apply to SWIFT or have only partial relevance. Six of the ten Core Principles relate to typical risks in payment systems and for system participants (e.g. financial risks through participation, prompt final settlement, multilateral netting, the settlement asset, etc.). These Core Principles do not apply to SWIFT as it is not a payment system. With some degree of reinterpretation, other Core Principles can be relevant to SWIFT. For example, having a sound legal basis, proper access criteria or governance arrangements, are also issues of interest to the overseers of SWIFT. One of the ten Core Principles concerns Security and Operational Reliability, and this objective is indeed very important for a society like SWIFT. Overseers recognised that their main focus when overseeing SWIFT should be on operational risk, as this is believed to be the primary risk category through which SWIFT could pose a systemic risk to the global financial system. Operational risk is the risk that deficiencies in information systems or internal controls, human errors, or management failures will cause or exacerbate other types of risk.

(1) Core Principles for Systemically Important Payment Systems, CPSS, January 2001.
Recommendations for Securities Settlement Systems, CPSS, November 2001.
Assessment methodology for "Recommendations for Securities Settlement Systems", CPSS, Nov 2002.
Recommendations for Central Counterparties, CPSS, November 2004.
Central bank oversight of payment and settlement systems, CPSS, May 2005.

Overseers also reviewed alternatives to this approach. As SWIFT is in fact an IT (Information Technology) operations company, overseers could possibly rely on existing IT security framework methodologies, or be satisfied that SWIFT demonstrates compliance with IT security baselines considered to be "best practices" in the industry.

Overseers did not adopt these alternatives for 3 reasons. First, it was felt that overseers should themselves draft their expectations vis-à-vis SWIFT, in a wording relevant to both central banks and to the SWIFT Board and senior management, without having to choose arbitrarily between potentially equivalent methodologies used in IT operations companies. Second, by drafting high level expectations for the oversight of SWIFT, central banks emphasise the importance they attach to the good functioning of SWIFT while clarifying their objectives to various stakeholders. Stakeholders that were identified are SWIFT itself, the SWIFT Board, the SWIFT Technical Oversight Group (TG) that is receiving additional guidance from the senior level overseers, and the non-G10 central banks and other public authorities not involved in the actual oversight on SWIFT but having a legitimate interest in the smooth functioning of SWIFT operations. A third reason for issuing high-level oversight expectations vis-à-vis SWIFT, rather than more detailed, prescriptive standards, is that in this way overseers leave SWIFT maximum flexibility to demonstrate compliance with the expectations, without too much interference in SWIFT's existing risk management processes and reporting frameworks. Overseers want to remain neutral in terms of the chosen processes and frameworks in use at SWIFT, but are offering, via the High Level Expectations, a platform which SWIFT can use to discuss with overseers the risks and risk management processes that are relevant to central bank overseers.

The SWIFT Cooperative Oversight Group has thus decided to develop a specific set of principles, different from the Core Principles, that it would apply to SWIFT, and in which it will go into more detail on various dimensions of operational risk.

2. The five High Level Expectations for the oversight of SWIFT

The overseers' focus on SWIFT's management of operational risks has been translated into five High Level Expectations (HLEs). Two HLEs focus on the management of risks (HLE 1, Risk Identification and Management; HLE 5, Communication with Users) and three HLEs deal in more detail with specific types of risk that should be managed (HLE 2, Information Security; HLE 3, Reliability and

Resilience; HLE 4, Technology Planning). Annex 1 provides the full text of the five HLEs. We will be discussing briefly each of the five HLEs in the remainder of this section.

"Expectation" means "what objectives overseers expect SWIFT to meet". The expectations are phrased at a "high level" as overseers do not want to be prescriptive about how SWIFT should achieve the stated objectives. These expectations should not be seen as "industry best practices" that overseers expect SWIFT to follow. Indeed, given that a large and growing number of participants, including systemically important systems, depend on SWIFT's core messaging service, and given the degree of SWIFT's criticality to the functioning of such payment systems, industry best practices might be insufficient, as SWIFT will be expected to go beyond such practices. Moreover, "best practices" very often are industry specific as well as relative to a firm's size and importance. SWIFT's activities do not necessarily compare easily to those of other service providers or market infrastructures.

The High Level Expectations are directed at SWIFT's critical services, i.e. the two core components of its messaging services, FIN and SWIFTNet. FIN is SWIFT's financial messaging application. It runs on SWIFTNet, SWIFT's advanced Internet Protocol (IP)-based messaging platform. SWIFTNet comprises a portfolio of services and products that enable customers to communicate mission-critical financial information and transactional data securely and reliably. FIN and SWIFTNet are the critical services that are used by systemically important payment systems and securities clearing and settlement systems, and for correspondent banking activities. SWIFT activities that are not critical to the smooth functioning of the financial system (e.g. because of a small market share) are outside the scope of the central bank oversight of SWIFT, so that overseers' expectations vis-à-vis SWIFT do not apply to such products and services.

HLE 1 Risk Identification and Management

The overseers' high level expectation is that SWIFT has put in place processes for risk identification and management, is implementing controls to manage the identified risks, and has procedures in place to periodically reassess risks and to react to changed risk profiles or risk acceptance levels. The involvement of the Board and senior management in risk assessment and management processes as well as the independent, professional functioning of an internal audit organisation are subjects for review. Risk management practices in various specific domains are reviewed in more detail, e.g. the management of third party dependencies and the impact of strategy decisions on the critical services.

HLE 2 Information Security

The overseers' high level expectation is that SWIFT appropriately manages information security risks, i.e. maintaining the confidentiality and integrity of information which it processes, and guaranteeing the availability of its critical services. Processes for monitoring compliance with the information security policy, for capacity planning or for change management are reviewed to determine whether this expectation is met. A well-known industry information security standard is ISO 17799. ISO 17799 is actually a comprehensive set of controls comprising best practices in information security. Each of the domains referred to in the ISO 17799 information security standard is also contained in the overseers' use of the term "information security". However, two aspects have been isolated from the current definition of information security, and are covered in HLEs 3 and 4: business continuity management is dealt with under HLE3, reliability and resilience, and some aspects of building security into applications during information systems acquisition, development and maintenance, are covered by HLE 4, technology planning.

The notion of "confidentiality" in an information security context refers to the controls in place to help ensure the protection of sensitive information from unauthorised disclosure. This confidentiality concept in the context of the functioning of IT systems is different from what data protection authorities might also define as confidentiality, i.e. preventing personal data from being passed on or disclosed without the prior consent of the person involved. The overseers' definition of confidentiality relates to the functioning of IT systems, not to data protection, an activity which is outside the scope of the oversight mandate and which has been entrusted to other authorities.

HLE 3 Reliability and Resilience

A major focus of the SWIFT oversight activities is to obtain assurance that SWIFT critical services are reliable and resilient. As reliability and resilience of SWIFT services are so crucial, a separate High Level Expectation focusing on this aspect was introduced. The overseers' high level expectation is that SWIFT ensures that its critical services are available, reliable and resilient, and that SWIFT has appropriate business continuity management and disaster recovery plans designed to support that. Plans should be tested periodically, including with customers, and operational incidents should be adequately reported and analysed, as they might be an indicator of flaws that could potentially have much wider implications.

In recent years, overseers have focused closely on discussing with SWIFT whether and how it is meeting this high level expectation, precisely because of SWIFT's critical role in the global financial system. These reviews will presumably continue to constitute a major SWIFT oversight focus in the years to come.

HLE 4 Technology Planning

The overseers' high level expectation is that SWIFT has in place robust methods to plan for the entire lifecycle of the use of technologies and for technology selection. Effective technology planning reduces the risk that SWIFT is constrained by dependence on legacy technology and might result in a more flexible technology platform that allows SWIFT to adapt its systems more rapidly and more cheaply.. Overseers are interested in technology planning because it should make risk-reducing measures easier to implement and ensure vendor support is available, enhancing operational performance. There are several other motivating factors behind this oversight expectation. The criticality of the SWIFT services is one reason, the specific SWIFT "ecosystem" is another. There are more than 8000 SWIFT customers, ranging from very big to small, geographically spread over more than 200 countries, in both developed and emerging economies. As the technology chosen by SWIFT in its client-facing services may impact on the technology risks faced by its users, the final choice has to be robust and sufficiently mature.

HLE 5 Communication with Users

The overseers' high level expectation is that SWIFT provides sufficient information to its users to make sure that these users clearly understand their role and responsibilities when using the SWIFT services, enabling them to manage adequately the risks related to their use of SWIFT.

The overseers review the way in which SWIFT consults with its major users on technology choices for its critical services. SWIFT needs to consider the risks to users of the changes it is making. The adequacy of procedures for crisis communication and mechanisms for customer feedback on operational risks are also discussed.

3. Use made of the High Level Expectations for the oversight of SWIFT

The SWIFT Cooperative Oversight Group started developing the HLEs in 2005 and invited feedback from SWIFT on consultative versions before finalising them in 2006. The publication of the HLEs provides transparency on the SWIFT oversight objectives for both SWIFT and the general public.

First, the HLEs provide the basis on which SWIFT is expected to prepare its self-assessment. With such self-assessment against the HLEs, SWIFT is reporting within a framework specifically set up for addressing central banks' oversight concerns vis-à-vis SWIFT, satisfying central banks' information needs from a financial stability perspective. Such self-assessment would not represent the opinion of the overseers, but SWIFT's own assessment of how it lives up to the HLEs.

It should be noted that this SWIFT self-assessment against the HLEs caters for a different need (audience of central banks; discharge of oversight and financial stability obligations) than the SAS 70 Type 2 report that is prepared by SWIFT and its external security auditor. The SAS 70 report on Information Security describes the SWIFT control objectives, the controls that are in place, and the outcome of tests of controls by the external security auditor in the domains of confidentiality, integrity, availability, governance and change management. This report is intended for the SWIFT users, as well as their auditors. Overseers value the SAS 70 report and the audit processes in preparation of the report as an integral part of SWIFT's security control awareness culture.

The HLEs also provide a framework within which the overseers can organise their activities. In the oversight of SWIFT, activities are set up in two layers: a senior level, that interacts with SWIFT in high-level and policy discussions, and a technical level, the SWIFT TG, that conducts the technical oversight fieldwork, reports to the senior oversight level, and takes guidance from the latter in organising and prioritising its technical oversight activities.

The HLEs are providing SWIFT and overseers with a common language, a framework within which discussions can be held. Hence, the TG's risk-based oversight planning methodology has been reviewed and now builds upon the HLE framework. This modified SWIFT oversight methodology is being implemented from 2007.

It should also be noted that the introduction of the HLEs and the discussions that will take place between overseers and the SWIFT Board and senior management within the framework built by these HLEs are not replacing the groundwork of the central bank oversight. The overseers will continue to identify specific topics for review and discussion with SWIFT management and Internal Audit. Nor does the HLE framework confine the discussions that can be held between overseers and SWIFT to the topics addressed in the HLEs. A good example is governance. HLE 5, Communication with Users, touches upon user governance, but overseers' interest in proper SWIFT governance arrangements are broader and they have deliberately remained out of the HLEs. In fact, the HLEs are establishing a framework taking properly functioning governance arrangements as a pre-conditional environmental prerequisite. This review of governance arrangements is conducted as a separate activity by the overseers.

Annex

High Level Expectations for (the Oversight of) SWIFT

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.

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.

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.

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.

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 SWIFT's own operations, or, alternatively, techniques SWIFT uses to prevent any such user impact on SWIFT 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.