Gottfried Leibbrandt
Chief Executive Officer

18 Febrruary 2014
GL/ddh

To the attention of:

The Committee on Payment and Settlement Systems
and
The International Organization of Securities Commissions

By email to the CPSS secretariat (cpss@bis.org) and to the IOSCO secretariat (annexf@iosco.org)

Subject: Response to the CPSS-IOSCO consultative report "Principles for Financial Market Infrastructures: Assessment methodology for the oversight expectations applicable to critical service providers".

Dear Sir, Madam;

SWIFT thanks the Committee for the opportunity to respond to the Consultative Report on the *Assessment methodology for the oversight expectations applicable to critical service providers*.

We believe that the development of such an international framework is of paramount importance, and are grateful for the opportunity to input to its finalisation. Just as the Committee's "*Principles for Market Infrastructures*" are designed to serve as internationally accepted standards for market infrastructures, we believe it is vitally important that there be internationally accepted standards for the assessment of Critical Service Providers ("CSPs"), and that these are both applied and accepted on a consistent basis across jurisdictions.

Much like market infrastructures, many CSPs either offer cross-border services directly, or are providers to market infrastructures, which in turn offer cross-border services. In developing and eventually promoting this assessment framework, the CPSS is helping to ensure not only that market infrastructures and their CSPs are upheld to high standards, but also that such standards will be accepted universally. On this note, we would observe that national and regional authorities (i.e., NIST[1] in the United States), are increasingly looking to develop their own measurement frameworks which would apply to CSPs. We would urge the Committee to advocate for the global adoption of a single framework and form of categorisation to avoid duplication and or conflict between different forms of measurement and categorisation.

SWIFT has read the consultation with great interest, and supports the key questions covering the five oversight expectations for CSPs. We would, however, observe that additional questions may need to be incorporated over time to ensure that the assessment captures all relevant developments. We would therefore urge the Committee to ensure that the incorporation of any additional questions is done in a timely and coordinated manner, perhaps via an annual review process. At the same time, and in the interest of maintaining a level playing field, we believe it is important that the Committee strongly discourage market infrastructures and their supervisors from unilaterally expanding the scope of their assessments.

[1] National Institute of Standards and Technology www.nist.gov

S.W.I.F.T. SCRL
Avenue Adèle 1,
B - 1310, La Hulpe
Belgium
T +32 2 655 4073
E gottfried.leibbrandt@swift.com
W www.swift.com

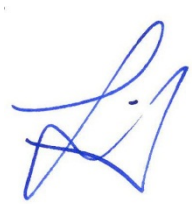
VAT BE 0413.330.856 - RPM Nivelles

To achieve the full benefit of the framework set out by the CPSS and to avoid duplication, it will also be necessary to ensure that the assessment of a CSP's adherence to the expectations is not only evidenced, but also that it is accepted both by market infrastructures and by their supervisors. In this respect the Consultation asks how a CSP's compliance with the Principles should be assessed. In our view CSPs should generally be able to evidence their service level compliance by providing the results of their own internal assessment processes, provided of course that these cover the key questions for each of the five oversight expectations. We would further recommend that the Committee use this opportunity to encourage CSPs to undertake external assessments; for instance, the Assessment Framework could set out that any such independent external assessments should serve as verifiable evidence of compliance with the expectations.

Again we thank you for the opportunity to comment on the proposed Assessment Framework. We hope that the above, together with the more detailed comments set out in the annex to this letter will be useful to you in finalising the proposed assessment methodology.

Should you wish to discuss our comments further, please do not hesitate to contact Peter De Koninck (peter.dekoninck@swift.com) who will coordinate any such discussion on our behalf.

Yours sincerely



Copy: National Bank of Belgium, Lead Overseer of SWIFT

Background

SWIFT is a member-owned, cooperative society headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholding Users, comprising over 2,300 financial institutions. We connect over 10,500 connected firms, across more than 210 territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides market infrastructures, banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

Detailed Comments

1) Applicability of Annex F;

SWIFT provides critical services to a wide range of organisations that are financial market infrastructures (FMIs), as defined by the CPSS-IOSCO Principles. As stated in our letter of 28 July 2011 in response to the original consultation on the Principles we strongly welcome all efforts to ensure that the operations of all FMI critical service providers are held to a consistent standard.

As such, we believe that Annex F should apply to all external and internal providers of critical services, in order to ensure the objective of controlling systemic risks is properly met and to ensure fair competition between the parties.

2) Reporting;

SWIFT supports the proposed key questions which have been included in the consultation. As drafted, we believe these questions will provide a solid basis upon which an assessment of a CSP's compliance against the five oversight expectations in Annex F can be made. We recognise that these questions may need to change over time. If so, this should be done in a coordinated manner led by the Committee, ideally via an annual review process. (Further comment in this respect is set out in point (4) below).

Individual market infrastructures and their competent authorities should be discouraged from unilaterally adding additional questions to the assessment or extending the scope of the assessment.

3) Type of Assessment;

CSPs should be permitted to evidence their compliance with the five oversight expectations by producing self-assessment responses to the questions outlined in the consultation. We believe the Committee should encourage CSPs to undergo and provide external assessment of their compliance. To encourage this development, the Assessment Methodology could explicitly recommend that such independent external assessments should serve as verifiable evidence of a CSP's compliance with the principles.

4) Completeness of the assessment framework;

While we fully understand the challenges of creating a framework that will cater to the needs of all stakeholders, the statement in the introduction that: "R*egulators, supervisors, and overseers of FMIs could, at their discretion, pose additional questions as needed to address the particulars of the FMI, its critical service providers, or other relevant issues.*" creates uncertainty and makes it impossible for CSPs to plan for timely, complete and accurate responses.

Whilst we recognise that revisions to the assessment questionnaire will be needed over time, we strongly urge the Committee to ensure this is done on a consistent and coordinated basis. Ideally this would be done no more frequently than once a year with any additional questions or scope agreed through the Committee. The introduction of ad hoc questions or expansion of the assessment will undermine the Committee's objectives, create an unlevel playing field, make the process less efficient and inhibit meaningful comparisons between FMIs and their CSPs in different markets.

5) Confidentiality of Reports;

To help ensure an appropriate level of transparency, but to avoid security concerns, SWIFT strongly believes that a CSP's self-assessment or external assessment should remain confidential and be restricted to relevant market infrastructures and their competent authorities, while allowing for appropriate international cooperation through the CSP's competent authority.

6) Recipients of Reports;

We would welcome additional guidance on who should be receiving the CSPs' reports – while initially it appeared that such reports would be for the market infrastructures themselves, the assessment framework now seems to indicate that various other parties may need to receive these reports e.g., the market infrastructures' supervisors. Given the potential confidentiality issues, the list of potential recipients should be determined up front – ideally in the Committee's assessment framework. Further, we believe that the communication process should be streamlined to ensure all stakeholders have access on a need-to-know basis, perhaps by means of a central repository with controlled access to ensure confidentiality of the reports.

7) Proposed Amendments

7.1 Q 2.7 states:

"*How does the critical service provider ensure that all employees and relevant external parties are made aware of their responsibilities and liabilities, and of security threats, as defined in the information security framework?"*

In order to ensure the appropriate calibration of this requirement, we recommend this be amended to read:

"*How does the critical service provider ensure that all employees and relevant external parties are made aware of their responsibilities and liabilities, and of* ***relevant*** *security threats, as defined in the information security framework?"*

7.2 OE1. Risk identification and management, states:

"*A critical service provider should have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept certain risks."*

To cater for those CSPs that offlay some of their related risks in the insurance market, we recommend that this be amended to read:

"*A critical service provider should have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept* ***or transfer (e.g. insure)*** *certain risks."*

7.3 OE 3 Reliability and resilience, states:

"*Any operational incidents should be recorded and reported to the FMI and the FMI's regulator, supervisor, or overseer."*

To lessen the likelihood of FMIs and their supervisors receiving reports on insignificant incidents, we propose that this be amended to read:

"*Any* ***critical*** *operational incidents should be recorded and reported to the FMI and the FMI's regulator, supervisor, or overseer."*

ENDS