



SWIFT response to the
CPMI-IOSCO consultative report on
“Cyber resilience of financial market
infrastructures”

23 February 2016

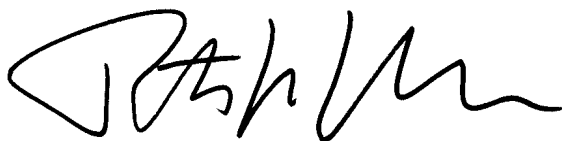
SWIFT welcomes the CPMI-IOSCO consultative report providing additional guidance on how financial market infrastructures (FMIs) can strengthen their cyber resilience, and we appreciate the important work CPMI-IOSCO is doing to enhance the stability of the financial system. While SWIFT¹ is not an FMI, we certainly are a critical service provider to the financial industry and we fully understand our responsibilities in helping to achieve the overall resilience of the financial system and the broader economy.

SWIFT believes that the report provides a good, comprehensive high-level framework for creating and evaluating a cyber-resilience programme. Having established a mature cyber resilience programme ourselves, and based on our interaction with many parties in the SWIFT eco-system, we understand the importance and the challenges of establishing a common language and it comes as no surprise that some of the terminology used in the consultation paper is not fully aligned with our own practices. We believe, however, that any differences in terminology can be resolved easily and do not require changes to the paper.

Regarding the points made on “learning and evolving”, we believe that the identification of “lessons learned” after each detected exposure is essential in helping any organisation to improve its stance towards cyber resilience. At SWIFT we see this as a distinct “phase” after each incident, in addition to the learning and evolving that is part of every step of the process.

We also appreciate that the guidance allows each organisation to apply the principles to its own context, unique cyber threats, and risk appetite, although the document is surprisingly prescriptive regarding the resumption (of critical operations) within two hours of disruption. Recovery from an outage within two hours may be a laudable long-term objective for any participant in the industry, and there are many scenarios from which recovery within a two hour period is feasible. However, there are also scenarios for which this recovery time objective is unrealistic, particularly in complex cyber scenarios where the detection of the problem can, on average, take 200 days, according to industry statistics.. In some instances it may even be an undesirable objective, as reopening service too quickly could promulgate a cyber issue through the financial system.

We thank CPMI-IOSCO again for the opportunity to contribute to this important dialogue.



Peter De Koninck
Chief Auditor | SWIFT
Tel: +32 2 655 4217
Mob: +32 474 990 958

¹ 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 3,000 financial institutions. We connect over 10,800 connected firms, across more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes. SWIFT provides 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.